Dear Sir/Madam,
Firstly, because the cover sheet you request and also your other request for submissions to be in Word format, I'm afraid that you will have to make do with this submission in this form.
As a Linux user I do not have access to Microsoft products. May I suggest that for your next and future consultations, that you provide documents in an open format and that you accept submissions also in open format.
My name is Michelle Knight I would be grateful if this letter could be taken in response for the consultation on the digital rights act and associated issues.
I have a number of concerns which dovetail together.
Firstly, asking ISP's to police a transaction which they have no legal authority to properly examine, is destined to failure. Deep Packet Inspection violates privacy issues and is currently against the law. It is therefore concerning that Virgin have already been running their experiment examining customers packets.
This raises questions of not only why Virgin have not been brought to book for deep packet inspection but also that if DPI is allowed, (unlikely given Europe's privacy position) it is easily circumvented by using encryption. To decrypt packets on-the-fly, as would be necessary, is a game of cat and mouse that would never be won as consumer processing power would increase at a similar ratio to that available to ISPs at reasonable cost.
It is not acceptable for any corporation to think that they have the right, or that it is possible for them to be granted the right, to examine peoples personal communication streams.
The cost of this process would also be born by the ISPs customer base and the taxpayer. To engage in such a wasted process would cost the country dear and as far as I can see, would be politically impossible to justify the British public footing an expensive technical bill on a failed process, for what should be civil proceedings brought by the entertainment companies concerned at their own expense.
The level of proof required at present for a customer to be held of a degraded status is not socially acceptable. With the amount of Internet traffic in to a household rising, a simple comparison of an entertainment companies claim against the traffic being consumed by the customer on a particular day, is not socially acceptable as proof to hold a person as being guilty of a crime.
This situation is compounded by the state of wireless security in our current age. It is for a court of law to determine someone a criminal, not an ISP or an entertainment company.
Last year saw the successful attack of WPA-TKIP, seeing weak passwords fall in three minutes when run against a prepared dictionary database. This leaves WPA-AES as the only secure consumer wireless security available. With the "n" series wireless allowing ranges of 70 metres indoors and in excess of 200 metres outdoors, any would be hacker can sit back at a safe distance in a property several houses away from their intended victim.
MAC address black/white lists easily fall to any hacker; simply listen to the traffic and then spoof any client MAC address seen on that channel. Not that MAC address filtering is enabled by default on any consumer wireless router that I know of.
There is the question of routers that come to the customer pre-programmed by the ISP themselves; how dare the ISP then hold the customer responsible for any breach of security on a wireless system that they have not only programmed, but also locked the customer out of.

With some systems and routers being unable to communicate properly at the higher security settings (PS2 and some Belkin equipment among them) the customer has no other way forward than to lower the security settings and leave themselves open to attack.
There is also the question of how is the average consumer supposed to know the difference between WPA, WEP, TKIP, AES and the rest of it. The average consumer won't have a clue, which is what led to the ISP's pre-configuring the units for them in the first place.
Bad practice by manufacturers and ISPs are responsible for gaping holes in consumer wireless security and the consumer is then held responsible for this. It is an unacceptable situation and needs Ofcom to correct this.
Our communications systems are not secure. Even on the subject of mobile phone communications there is the following taken from an article on The Register at this address - http://www.theregister.co.uk/2010/07/29/cell_phone_snooping/
Quote
“The whole topic of GSM hacking now enters the script-kiddie stage, similar to Wi-Fi hacking a couple years ago, where people started cracking the neighbor's Wi-Fi,” said Karsten Nohl, a cryptographer with the Security Research Labs in Berlin who helped spearhead the project. “Just as with Wi-Fi, where they changed the encryption to WPA, hopefully that will happen with GSM, too.”
The suite of applications now includes Kraken, software being released at the Black Hat security conference on Thursday that can deduce the secret key encrypting SMS messages and voice conversations in as little as 30 seconds. It was developed by Frank A. Stevenson, the same Norwegian programmer who almost a decade ago developed software that cracked the CSS encryption scheme protecting DVDs.
End Quote
A move to complex certificates should be considered. This need not be overly complex; an SD or Micro SD card slot on the router should enable it to write its certificate to the card at the touch of a button. The client device, mobile phone, PC, console, etc. should then be able to read it in from said memory card. Wireless security could thus be taken in to the world of certificates and actually make the process far simpler for the consumer than it is now.
It is impossible to escape the fact that the entertainment industry has long had an image in the UK of being a legal criminal; the charges for media in the UK being double some other European countries in recent years. It is not socially acceptable for public money and effort to be spent in trying to uphold an out date business model practiced by companies that have been considered to be over charging the UK consumer for many years.
Indeed, the actions of Sony and other corporations that distributed music CD's with root kit software which illegally installed itself without permission on to customers computers, is an indication of the contempt with which these companies hold their legitimate, legal, paying customers; yet I haven't seen these corporations being prosecuted by the UK for these actions.
It is time for this country to stop spending public money and holding its own citizens as criminals on the basis of the entertainment companies say-so; especially after their behaviour in the market place and the poor state of security on consumer equipment.
Treatment of software piracy should be dealt with on the same basis as many other campaigns, public education and awareness as was done with drink driving for example. However, for this to work it would require the entertainment companies to treat their customers with respect and unless these entertainment corporations show

willingness to come half way across the bridge, public money should not be spent on their cause.
Yours sincerely,
Miss Michelle Knight