

## THE IDENTIFIED EMERGING POLICY RESPONSES

### 1. INSERT

#### *Traffic shaping*

2. The UK Parliament is presently considering introducing technical measures “to tackle the problem of unlawful peer-to-peer (P2P) file-sharing”. This proposal (as it is presently expressed) would grant the regulator, Ofcom, the power to oblige ISPs to apply certain technical measures against repeat offenders if **other, non-technical, measures prove to be deficient in reducing infringement**.<sup>1</sup>
3. Some of the technical measures presently under consideration are methods of traffic shaping, namely bandwidth capping and bandwidth shaping<sup>2</sup>.
4. Bandwidth capping and bandwidth shaping are defined in the *Digital Britain – Final Report* respectively as:
  - “capping the speed of a subscriber’s Internet connection and/or capping the volume of data traffic which a subscriber can access”; and
  - “limiting the speed of a subscriber’s access to selected protocols/services and/or capping the volume of data to selected protocols/services.”<sup>3</sup>

For the purposes of this paper, we will use these definitions.

5. **In some jurisdictions [places other than Australia?], such as Australia, ISPs routinely employ bandwidth capping, shaping or a combination or both to manage services provided to subscribers. For example, subscribers may have a choice of Internet access plans with different volume caps and/or speed caps. In some cases, speed is slowed after a volume cap is reached. In other cases, subscribers are charged a higher price to download data in excess of the volume cap.**

**What methods of copyright infringement and/or infringers is the policy designed to prevent or reduce?**

6. The policy is designed to reduce online copyright infringement via P2P protocols.

**How effective is the policy likely to be at preventing or reducing copyright infringement?**

**Vis-à-vis which methods of copyright infringement?**

**What solutions might infringers choose or develop in response? What impact would these have?**

---

<sup>1</sup> Government Statement on the Proposed P2P File-sharing Legislation at page 1 - <http://www.berr.gov.uk/files/file52658.pdf>

<sup>2</sup> *Digital Britain – Final Report* at pages 111-112  
[http://www.culture.gov.uk/images/publications/chpt4\\_digitalbritain-finalreport-jun09.pdf](http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf)

<sup>3</sup> *Digital Britain – Final Report* at pages 111-112  
[http://www.culture.gov.uk/images/publications/chpt4\\_digitalbritain-finalreport-jun09.pdf](http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf)

7. For the purposes of this discussion, except as otherwise stated, we have assumed that the subscriber is the infringer and will be aware when bandwidth capping or bandwidth shaping is applied. **As a matter of transparency and fairness, we consider it essential that the subscriber receives adequate advance notice.**

#### *Bandwidth shaping*

8. Capping data downloads will not affect a subscriber's ability to access the Internet until the total volume downloaded reaches the maximum allowed, and thus would not, of itself, prevent a subscriber from continuing to engage in online copyright infringement by P2P or any other means. It is possible that some subscribers, knowing they are restricted to a maximum download in a given period, may reduce their infringing activity, choosing to first consume their limited data allocation for perceived higher priority uses which are lawful. Such subscribers may be more likely to be casual infringers rather than repeat infringers **which this policy is not intended to address.**
9. Capping downloads without a corresponding cap on uploads would not prevent the subscriber from continuing to act as a seeder in a P2P network so long as downloads are kept below the threshold.
10. Whether capping the speed of a subscriber's connection will affect his or her ability to engage in online copyright infringement via P2P or any other means depends on the degree to which the speed is capped. To effectively prevent the subscriber from using P2P, the connection would need to be slower than what is required for any of the existing, or likely to be developed, P2P protocols. **Otherwise, it would only limit the amount of data that could be downloaded via P2P protocols within a given 24 hour period. [Is this figure known?]** Further, as P2P protocols often select their peers opportunistically, capping the speed may just shift infringement to another subscriber.
11. If upload speed is not sufficiently reduced, the cap on download speed may not prevent the subscriber from continuing to act as a seeder in a P2P network.
12. Even if capping data speeds prevented the subscriber from using P2P protocols, it is possible that the subscriber could still continue to engage in online copyright infringement by other methods which operate effectively at slower speeds (e.g. **insert example**). **However, it may also encourage the subscriber to access content legally.**
13. Once a subscriber reaches the maximum data threshold, he or she has several options **for accessing additional data**, with varying levels of associated cost and inconvenience: For example, the subscriber could:
  - **respect the imposition of the limitation;**
  - subscribe to another ISP (unless all other available ISPs were somehow prevented from supplying their services to the subscriber);
  - use another subscriber's connection with permission (friend, workplace, library, Internet café, etc) (less likely if this was prohibited by law);

- use another subscriber's connection without permission (e.g. accessing unsecured wireless connections);
- establish his or her own ISP.

Those options are also available to a subscriber whose connection has been slowed.

14. It may be impossible or, at best, resource intensive and expensive for a regulator to ensure that the subscriber does not have the ability to download data in excess of the imposed maximum volume or speed **via other connections**. However, it may make it more difficult or inconvenient for some infringers.

*Bandwidth shaping (volume and data)*

15. To be able to bandwidth shape P2P traffic separately, an ISP must be able to detect and differentiate P2P traffic from other traffic.
16. **Although the policy (as presently envisaged) does not distinguish between lawful and unlawful P2P traffic, an ISP could "white-list" lawful sources of P2P traffic and thus exempt them from bandwidth shaping.<sup>4</sup> However, given extra labour and cost involved in maintaining white-lists for subscribers who are subject to the policy, ISPs may be reluctant to offer that service to those persons.**
17. P2P traffic which uses known fixed port numbers is relatively easy to detect, however traffic can be transported using P2P using dynamic and random port numbers, thus making detection by using port numbers more difficult.
18. Another way unencrypted P2P traffic can be detected is via Shallow Packet Inspection, that is, through inspection of the header of a data packet, however, many P2P networks encrypt their traffic.
19. Various Deep Packet Inspection<sup>5</sup> ("DPI") techniques have been developed to detect encrypted P2P traffic (i.e. to recognise P2P traffic without seeing its contents), including techniques which analyse traffic behaviour. These techniques vary in their effectiveness.
20. The policy does not require an ISP to identify and distinguish between lawful and unlawful P2P traffic so for the purposes of deploying the policy it matters not whether the technological measures could break the encryption provided they can reliably detect P2P traffic.
21. As the content of the P2P traffic is irrelevant to the policy, subscribers subject to P2P bandwidth shaping may be more concerned about disguising the fact that they are sending or receiving P2P traffic than they are about encrypting its contents. However, having been detected as "infringers" which led to the application of the

<sup>4</sup> See Ipoque whitepaper on *Bandwidth Management Solutions for Network Operators* at page 2 <http://www.ipoque.com/userfiles/file/BW-Management-for-Operators-WP.pdf>

<sup>5</sup> DPI is "is the act of any IP network equipment which is not an endpoint of a communication using any field other than the layer 3 destination IP address for any purpose" (www.wikipedia.org)

policy (see paragraph 2), there may be a strong incentive for them to seek to disguise the contents.

22. Internet users who wish to disguise their P2P traffic from third parties have developed and are continuing to develop new methods to prevent third parties from detecting the fact they are they are using P2P protocols.
23. For example: Message Stream Encryption (“MSE”) protocol is intended to disguise BitTorrent P2P traffic by generating what seems to be a random header. It is also designed to work with RC4 (a stream cipher) to encrypt the contents.<sup>6</sup> However, more sophisticated traffic analysis tools are still able to detect P2P even where MSE and RC4 are used.<sup>7</sup> [What effect does MSE and RC4 have on the Internet (if any)?]
24. Another method used to disguise P2P traffic is to send P2P traffic via an encrypted virtual private network (VPN) tunnel which encapsulates the network traffic within encrypted packets between tunnel endpoints.<sup>8</sup> What effect does VPN have on the Internet (if any)?]
25. Apart from developing methods of disguising P2P traffic, infringers are also likely to develop means to prevent technical measures to prevent or reduce the effectiveness of bandwidth shaping. For example, Transmission Control Protocol (“TCP”) packet resets to delay P2P traffic such as BitTorrent, would not be effective against traffic transported using the uTorrent protocol which operates via the User Datagram Protocol (“UDP”). (As at 2008, BitTorrent Inc’s VP of Product Management estimated that 28 million unique users use uTorrent every month.<sup>9</sup>)<sup>10</sup> [How can P2P via UDP be throttled? \*UDP is delay sensitive]

#### **Are there any known technical flaws?**

26. [Insert details here as to whether there are any known technical flaws with traffic shaping?]

#### **Would the policy identify particular infringers? Which infringers? How?**

27. The policy is not designed to detect infringers, it is intended to be applied after infringers have been identified.

#### **What impact (if any) would the policy have on privacy?**

*Bandwidth capping*

---

<sup>6</sup> See *The Arms Race in P2P* Kevin Bauer, Dirk Grunwald and Douglas Sicker, University of Colorado at page 9 [http://www.tprcweb.com/images/stories/papers/kevinbauer\\_2009.pdf](http://www.tprcweb.com/images/stories/papers/kevinbauer_2009.pdf) and [http://www.azureuswiki.com/index.php/Message\\_Stream\\_Encryption](http://www.azureuswiki.com/index.php/Message_Stream_Encryption) and <http://en.wikipedia.org/wiki/RC4>

<sup>7</sup> See *The Arms Race in P2P* (above) at page 10

<sup>8</sup> See *The Arms Race in P2P* (above) at page 12

<sup>9</sup> <http://torrentfreak.com/utorrent-grows-to-28-million-monthly-users-081225/>

<sup>10</sup> See *The Arms Race in P2P* (above) at page 13-14

28. Technological measures which only “count” the volume of data received within a given time and then impose a technological cap should not reveal what content the subscriber is viewing, downloading and/or uploading.
29. Similarly, technological measures which only restrict the speed of a subscriber’s connection should not reveal the content of the data being streamed.

*Bandwidth shaping*

30. If P2P traffic is encrypted, technical measures employed to bandwidth shape that traffic should not reveal what content the subscriber is viewing, downloading and/or uploading. They may, however, by their very nature reveal information about the IP addresses used by the peers in the network. In some cases, such IP addresses, when combined with other information, could reveal personal information about the subscriber or other persons.
31. If P2P traffic is not encrypted, such technical measures may reveal the content and, thus, potentially reveal considerably more personal information about the subscriber, other peers in the network and/or third parties. For example: the subscriber may use unencrypted P2P to send a video of a family barbeque to other friends on the network.

32. [Check and more details]

**Is the policy proportionate to the harm it is designed to prevent or reduce?**

33. This is a difficult question. [INSERT]

**Would the policy discriminate against legitimate uses of applications?**

34. Bandwidth capping (as defined) would apply indiscriminately to all Internet use via the capped connection, including lawful and unlawful P2P activity. Some uses of the Internet require faster Internet connection speeds (e.g. video streaming and online games) and/or larger volumes of data traffic (e.g. software and video downloads). The extent of the impact this policy would have on legitimate uses of applications will depend greatly on the degree to which speed and volume are capped. However, any degree of bandwidth capping could affect the effectiveness and/or render a bandwidth-intensive application inoperable.
35. By contrast, bandwidth shaping (as defined) should only affect the targeted protocols – in this case, the P2P protocols used by P2P networks – **provided those protocols can be identified and distinguished from other traffic.**
36. Data exchanged through P2P file-sharing can be lawful or unlawful. Bandwidth shaping which cannot distinguish between lawful and unlawful file-sharing would prevent the user from using P2P for legitimate purposes. However, it should not affect non P2P internet use.

**Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols? If so, what would this mean?**

37. Bandwidth shaping focussed purely on the P2P protocol is unlikely to discourage or prevent the development of new communications protocols. The policy may in fact encourage development of new file-sharing protocols that would not be affected by the proposed bandwidth shaping techniques (e.g. uTorrent).

**Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?**

38. By their very nature, bandwidth capping and shaping at the subscriber level will impact the Internet architecture at the edge, since the edge requires that all traffic from a given subscriber must pass through a single point where it can be counted, capped, shaped etc. **Whilst that may be the case in any event, there is still a very clear tension between these technical measures and the desire of some users to have more reliable connections by having diverse routing.**

**What impact (if any) would the policy have on security?**

39. Bandwidth speed capping should not directly affect Internet security. However, a slower Internet connection may actually protect the subscriber from some bandwidth-hungry Internet security threats.

40. **Rate bandwidth shaping or capping will also make it slower or impossible to download Operating System patches, which could have a significant effect on the security of the subscriber's computer(s).**

41. Bandwidth shaping may encourage affected subscribers to encrypt data they send and receive because they may be concerned that the technological measures applied to effect bandwidth shaping may inspect the content of their traffic. Such subscribers would, therefore, apply a higher level of security to their traffic. Their demand for encrypted data may drive online service providers to support and provide encrypted traffic.

42. [insert]

**Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?**

43. The policy is unlikely to inhibit or enhance users' willingness to access the Internet, only their ability to do so. However, if the techniques deployed to bandwidth shape involve content inspection, users may be less willing to use the connection which is bandwidth shaped.

**Would the policy directly or indirectly reduce Internet access or the availability of Internet access?**

44. Bandwidth capping would directly reduce Internet access for all users of the affected Internet connection. The effect that capping the speed of traffic to and from a subscriber will have on that subscriber's access to the Internet and online services via that connection will depend on the degree to which the speed is capped and the services that individual wishes to use. **By contrast, provided P2P protocols can be successfully identified and distinguished from other traffic,** bandwidth shaping of P2P

protocols should only reduce access to content and services that use those protocols.

45. Capping the volume of subscribers' connections may have a greater impact on subscribers than capping the **speed** because most subscribers with an otherwise fast connection only use a fraction of the available speed.
46. As noted above, the affected subscriber (and other users of the affected connection) could, at least in theory:
  - subscribe to another ISP (unless all other available ISPs were somehow prevented from supplying their services to the subscriber);
  - use another subscriber's connection with permission (friend, workplace, library, Internet café, etc) (less likely if this was prohibited by law);
  - use another subscriber's connection without permission (e.g. accessing unsecured wireless connections);
  - establish his or her own ISP.
47. Nonetheless, all of these steps require the user to take positive steps to obtain alternate Internet access at greater inconvenience and cost.

**Would the policy materially raise or lower the costs of Internet access? To whom?**

48. If the subscriber for the Internet connection that is subject to bandwidth capping or shaping is required to continue to pay the same amount for Internet access, the policy would effectively cause the subscriber to pay more for Internet access. That person may or may not be the infringer.
49. The policy may directly increase ISPs' costs and may indirectly raise the costs of Internet access to other users if ISPs are required to purchase and/or develop the software **and hardware** needed to individually apply bandwidth capping and/or shaping. The cost is likely to be greater in the case of bandwidth shaping because of the complex tools required to analyse disguised and encrypted P2P traffic.

**Is there any risk of significant or material damage to third parties' (i.e. non-infringers) use of or access to the Internet? How?**

50. There is a real risk that the policy would limit innocent parties' access to the Internet – those individuals who are legally entitled to use the same connection as the infringer. Present bandwidth capping and shaping methods generally do not distinguish between users of the same connection. While it may be possible for ISPs to issue separate passwords for different users of the connection and thus different levels of Internet access, such a solution is unlikely to be attractive to regulators because passwords for non-restricted Internet access could be easily given to the infringer.

**Would the policy encourage or discourage the use of certain business models? If so, what would this mean?**

51. An application that moves large volumes of data, while being careful not to interfere with any other use, such as on-line file backup, is likely to be adversely affected by bandwidth capping.

52. [insert]

