# LINX Policy Briefing to Ofcom:
# Who is a "subscriber", who is a "communications provider"?
# And the interaction of these definitions with the "reasonable steps" defence for innocent subscribers

**Example business scenarios to be considered when drafting the Initial Obligations Code under ss.3-7 Digital Economy Act 2010**

*Prepared by Malcolm Hutty, Head of Public Affairs*


*The London Internet Exchange*
*Maya House, 134-138 Borough High Street, London SE1 1LB*
*Tel: 020 7645 3500 Fax: 020 7645 3529 Web: http://www.linx.net/*

## Applying the policy intent of the Act to its defined terms

From a purposive rather than legally analytical perspective, the challenge lies in applying the definitions in the Digital Economy Act to reflect the determination in the Act that technical measures should not be imposed without careful consideration by Ofcom, the Secretary of State and Parliament, while ensuring that subscribers cannot all avail themselves of immunity from the regime created simply by redefining their status at will.

If it was ever true that Internet access was usually available only in the home, that time has passed. Internet access is increasingly ubiquitous, and for good reason: it is becoming ever more deeply embedded in our society, and people increasingly expect Internet access to be made available to them wherever they are. Accordingly, the market has changed. Just as the monopoly of "the telephone company" previously gave way to a diverse marketplace of electronic communications networks and services, so assumptions about getting Internet access only from a dedicated ISP must give way to a recognition that end users enjoy Internet access from diverse sources; ultimately the Internet access is supported by a traditional ISP no doubt, but the end user is often served most directly by new forms of communications provider.

This paper identifies a number of cases where an organisation makes an Internet connection available to individuals; for example a school to its pupils, a hotel to its guests, a library to its readers or a pub to its drinkers. The question arises in each case as to whether the organisation is considered under the Act to be a "communications provider" or a "subscriber". This is significant both in understanding their responsibilities under the Act and also consequentially: if they are deemed to be "subscribers" their only protection under the Act would be in both proving that misuse was done by someone else and in implementing "reasonable steps to prevent other persons infringing copyright by means of the internet access service".

We are aware that some stakeholders argue that the term "communications provider" should be construed narrowly, in line with traditional market assumptions about electronic communications businesses, and so excluding most of these cases. These same stakeholders also argue that the "reasonable steps" defence should be construed as requiring the subscriber to take technical measures, such as deploying a firewall for content filtering or address blocking. This is no mere coincidence; the construction placed upon these two terms together fundamentally affects the implementation of the Act.

We believe that this is an unreasonable construction and, when the implications of both elements of this issue are considered together, it can clearly be seen that this construction would seriously compromise the policy balance Parliament struck. In many cases providers falling within the classes identified in this paper will be unable to offer unfiltered Internet access unless they are deemed to be "communications providers" under the Act; most of the remainder will be similarly handicapped unless "reasonable steps" is construed to be satisfied by measures other than technical measures. We do not believe that that is the outcome Parliament intended.

In passing the Act Parliament contemplated the possibility of imposing technical measures and recognised the danger of doing so, of "throwing the open and innovative Internet out with the copyright infringing bathwater". If Internet access were only readily available through tightly controlled, filtered gateways then the deployability and commercial viability of innovative Internet applications and services would be severely threatened. By rejecting calls to move straight to the imposition of such measures across the board, Parliament demonstrated that it understood and accepted this point.

Under the Act Parliament established carefully staged steps before technical measures can be introduced, each with important and powerful safeguards. These steps determine not only whether technical measures can be introduced, but also provides a check on *what kind* of technical measures can be required, for example whether the imposition of filtering is ever justified. In enacting these safeguards Parliament demonstrated that it did not yet agree that the level of copyright infringement, however serious, justified the widespread imposition of technical measures of the kind argued for by some stakeholders. The legislative record, and the government's own assurances that it hoped technical measures would never be necessary, both support this view.

It would therefore thwart the will of Parliament to construe the terms "communications provider" and "reasonable steps" so narrowly that in most circumstances the end user was unable to access the Internet except via a connection that was subject to technical measures that a third party intermediary was effectively required to impose under the Act by virtue of the narrow construction placed upon those terms. If in so many classes of Internet provision, as identified in this paper, the provider is deemed to be a subscriber, and if it were therefore effectively required to introduce the technical measures about which Parliament was so cautious, the market would be left devoid of Internet access without technical measures in all circumstances save only the special case of the domestic user's own home. This is not the policy balance Parliament struck.

Such a narrow interpretation is also unlikely to reflect a natural reading of the term "communications provider", and so may fail as a matter of law. It also risks failing to be compliant with Articles 12 & 15 of the E-Commerce Directive, or with the requirements of Article 1.3a of the Telecoms Framework Directive (as amended in 2009).

Happily, the Act does not require Ofcom to adopt an Initial Obligations Code that takes such an extreme position. s124A(4) of the Communications Act, which is inserted by s.3 Digital Economy Act, provides that

> "An internet service provider who receives a copyright infringement report must notify the subscriber of the report *if the initial obligations code requires the provider to do so*."

This appears to allow Ofcom discretion as to the circumstances in which an Internet Service Provider who receives a copyright infringement report would be obliged to notify the subscriber.

This reading is reinforced by s124C, which includes the following:

"(3) The provision that may be contained in a code and approved under this section includes provision that—

(a) specifies conditions that must be met for rights and obligations under the copyright infringement provisions or the code to apply in a particular case; "

We therefore recommend:

- That Ofcom provide guidance on circumstances that entitle a person to be considered a "subscriber", a "communications provider", and an "Internet service provider" under the Act; and
- That, when considering these definitions, the specific conditions referred to in s124C(3)(a) and the guidance to the First Tier Tribunal, Ofcom have due regard to the apparent intention of Parliament that technical measures should not be imposed without various safeguards, including further Parliamentary authority; and
- That it is stated clearly and formally in the Initial Obligation Code and in the terms of reference for appeals before the First Tier Tribunal that the "reasonable steps" required of innocent subscribers do not necessarily require the introduction of technical measures and could be satisfied, for example, through terms of use and other instructions to end users.

# List of groups of example scenarios



Note: these example scenarios are not intended as a comprehensive statement of all the relevant scenarios, nor are they intended to be a complete statement of the situations faced or issues raised for each of the identified classes. Instead, the intention is to raise questions as to the application of the key defined terms in the Act, by reference to selected real life examples. The classes chosen have been identified in an attempt to illustrate key distinctions that may be relevant to the interpretation of the definitions. In practice, particular cases may sometimes include circumstances that show overlaps with other classes.

## *Group A: Base cases*

| Scenario A1.: Residential consumer fixed-line Internet access | |
|---|---|
| **Situation:** | An individual obtains DSL Internet access in their own home from a commercial ISP as a customer of that ISP for their own domestic use.<br><br>The ISP operates their own network, including acquisition of IP addresses from an RIR, allocation of IP addresses to customers, routing, access control and the contractual and billing relationship. |
| **Anticipated Ofcom Guidance:** | The customer is a "subscriber". The ISP is an "Internet access provider". |

| Scenario A2.: Residential non-consumer fixed-line Internet access | |
|---|---|
| **Situation:** | An individual obtains DSL Internet access in their own home from a commercial ISP[1] as a customer of that ISP. The customer uses the Internet access to work from home, or otherwise in the course of business. |
| **Anticipated Ofcom Guidance:** | The customer is a "subscriber". The ISP is an "Internet access provider". |

| Scenario A3.: Non-residential business fixed-line Internet access | |
|---|---|
| **Situation:** | A company obtains Internet access[2] for its own office. The Internet access is used by its own employees and guests. Although the company's customers may use the Internet access incidentally when visiting the office, it is not part of the company's business model to provide Internet access to its customers.<br>For example, a firm of accountants. |
| **Anticipated Ofcom Guidance:** | The company is a "subscriber". The ISP[3] is an "Internet access provider". |

[1] The commercial ISP in this scenario is assumed to have the same characteristics as in scenario A1

[2] The commercial ISP in this scenario is assumed to have the same characteristics as in scenario A1

[3] The commercial ISP in this scenario is assumed to have the same characteristics as in scenario A1

| Scenario A4.: Business access from multiple locations | |
|---|---|
| **Situation:** | A company obtains Internet access for its own office. Multiple office locations are linked via private circuits or an ISP managed VPN service. |
| **Anticipated Ofcom Guidance:** | The company is a "subscriber". The ISP[4] is an "Internet access provider". All complaints against the company will be added to a single tally. |

| Scenario A5.: Commercial wi-fi hotspot ISP | |
|---|---|
| **Situation:** | A commercial ISP[5] operates a wi-fi hotspot in a third-party retail location (e.g. a café or an airport lounge). The end user can obtain Internet from access by keying in their credit card details or by entering in an account password previously obtained from the ISP. Access control (RADIUS), branding, the contractual relationship, the billing relationship and routing are all provided by the ISP to the end user. The only involvement of the third party (e.g.airport) is to provide the ISP with a site to locate the hotspot access point device, and to allow the ISP power and communications connectivity to the device[6]. |
| **Anticipated Ofcom Guidance:** | The end user is a "subscriber". The ISP is the "Internet access provider". The third party is not involved in any way relevant to the Act. |

[4] The commercial ISP in this scenario is assumed to have the same characteristics as in scenario A1

[5] Except as noted, the commercial ISP in this scenario is assumed to have the same characteristics as in scenario A1

[6] Although we are loath to tie our identified classes to particular companies' products, for the sake of clarity it is worth noting that BT Openzone and T.Mobile Hotspots are major operators' products that we understand match this description.

## *Group B: Business use scenarios*

| Scenario B6.: Business access via multiple provision | |
|---|---|
| **Situation:** | A company obtains Internet access for ten separate office locations on ten separate DSL lines. These are all routed individually, not joined in a corporate network. |
| **Questions for guidance:** | Is the company a single subscriber, or are the ten DSL lines ten different subscriber accounts?<br>Should all complaints raised against the company be added together into a single tally, regardless of which DSL line the complaint was made about?<br>Note that if the company chooses to obtain each DSL line from a different ISP these will necessarily be considered ten different subscriber accounts and a single tally will not be possible. |

| Scenario B7.: Employer provides access at home to staff | |
|---|---|
| **Situation:** | A company contracts with a single commercial ISP to provide DSL access at ten different locations. These locations happen to be the homes of ten key employees.<br>The ISP may or may not know that these are residential locations; very commonly it would *not* know. |
| **Questions for guidance:** | Is the company a "communications provider" providing Internet access to its staff? Is the company a subscriber? Or are the individuals in their homes a subscriber for the purposes of the Act, even if they don't have a contract with the ISP?<br><br>If the company is a subscriber, is it a single subscriber covering all ten locations, or is each location a separate subscription? i.e. should all complaints made against each employee for use of the Internet at home be added together and held against the company? Does this depend on whether the ISP manages its customer accounts by location or by customer name?<br><br>In an alternative case where the customer contract is with the individual not the employer, but the company pays the bill direct to the ISP, does this affect the interpretation? Note that where the contract is with the individual the ISP will have no knowledge of any private agreement by the employer to reimburse the employee for the fees paid by the employee for Internet access. |

## *Group C: Community Internet access*

| Scenario C8.: Municipal wireless access | |
|---|---|
| **Situation:** | A local authority considers Internet access to be a general public amenity that supports economic development and its social objectives alike. It provides free wireless access to all.<br><br>Alternatively, a public benefit organisation, that may or may not be a registered charity, does so for with substantially the same motivation. |
| **Questions for guidance:** | Is the local authority (or charity) a subscriber or a communications provider?<br><br>Is the local authority (or charity) an Internet access provider? Is it obliged under the Act to identify its users and to record the allocation of IP addresses? |

## *Group D: Libraries and community centres*

| Scenario D9.: Library access | |
|---|---|
| **Situation:** | A public library considers Internet access to be a core part of its traditional mission as adapted for the modern world. It provides free use of PC terminals with Internet access to all library users and/or wi-fi access. |
| **Questions for guidance:** | Is the library a subscriber or a communications provider?<br><br>Is the library an Internet access provider? Is it obliged under the Act to identify its users, to record the allocation of IP addresses, and to collect and record sufficient contact information to be able to send out notices to user months later? |

## *Group E: Hospitality trade*

| Scenario E10.: Cafes and pubs | |
|---|---|
| **Situation:** | A pub provides free wi-fi access to its customers.<br>The pub obtains an ordinary DSL account from an ISP, and has itself installed an ordinary domestic wi-fi access point.<br>The pub makes no charge for this service; the apparent business benefit lies in the kind of clientele this service attracts, their willingness to stay in the pub drinking coffee during the quiet morning and mid-afternoon period etc.<br>Either the wi-fi access point is entirely open, or a password is displayed behind the bar or provided to customers on request. |
| **Questions for guidance:** | Is the pub/café a "subscriber"? Is the pub/café a "communications provider" or an "Internet access provider" or both?<br><br>If the pub is an Internet access provider, does the Act require the pub to start obtaining and recording the identity of its customers who use the wi-fi connection?<br><br>If an individual pub is not considered a communications provider, does this still hold true<br>• For a chain of pubs and cafes providing Internet access to thousands of customers at once?<br>• Where the availability of Internet access is a major part of the customer proposition, rather than merely incidental?<br>• Where the café takes positive steps to restrict access to customers who have bought a drink e.g. within the last hour?<br>• Where the café charges separately for a password to access the Internet? |

| Scenario E11.: Small hotels, free access | |
|---|---|
| **Situation:** | A hotel/guest house/Bed & breakfast provides free wi-fi access to its customers.<br><br>The hotel obtains an ordinary DSL account from an ISP, and has itself installed an ordinary domestic wi-fi access point. The hotel makes no charge for this service. The hotel does know the identity of its guests, but **cannot identify the user of a particular IP address**. |
| **Questions for guidance:** | Is the hotel a subscriber? Is the hotel a communications provider?<br><br>If the hotel is an Internet access provider, does the Act require the pub to start obtaining and recording the identity of its customers who use the wi-fi connection? |

| Scenario E12.: Small hotels, voluntary identification | |
|---|---|
| **Situation:** | A hotel/guest house/Bed & breakfast provides wi-fi access to its customers.<br><br>The hotel obtains an ordinary DSL account from an ISP. It has installed a wi-fi access point that asks its guests to identify themselves in order to obtain access. This information is stored and the assigned IP address is recorded. **The accuracy of the information provided is not corroborated**. |
| **Questions for guidance:** | Is the hotel a subscriber or a communications provider? Is the hotel an Internet access provider, and so obliged to send out warning notices under s3? |

| Scenario E13.: Hotels, controlled access for guests | |
|---|---|
| **Situation:** | A hotel provides wi-fi access to its customers.<br><br>The hotel obtains an ordinary DSL account from an ISP. It has installed a wi-fi access point that asks for a password. Passwords are available from hotel reception. The hotel records who is given which password, and the access point records which password is assigned which IP address. Together, **these records can provide a link between the end user's identity in the hotel records and the IP address used**. |
| **Questions for guidance:** | Is the hotel a subscriber or a communications provider?<br>Is the hotel an Internet access provider, and so obliged to send out warning notices under s3? |

| Scenario E14.: Hotel visitors | |
|---|---|
| **Situation:** | A hotel provides an open wi-fi access point in its lobby and conference rooms. The identities of attendees at conferences are not known to the hotel. |
| **Questions for guidance:** | Is the hotel a subscriber or a communications provider?<br>Is the conference organiser a subscriber?<br><br>Does it make a difference that the availability of wi-fi Internet access is considered essential by conference organisers when choosing a venue?<br><br>Does it make a difference that a particular hotel may Internet access to many thousands of conference guests a year? |

## *Group F: Schools*

| Scenario F15.: School access | |
|---|---|
| **Situation:** | Access to the Internet is considered an essential part of education. Most schools therefore provide proxy-filtered Internet access to their pupils, often through a network supplied by their local authority or Regional Broadband Consortium (RBC). In these arrangements IP addresses will generally be 'owned' by the authority or consortium, though (for child protection and data protection purposes) only the school may be able to identify which pupil was using a particular IP address at a particular time. Many authorities run, or sub-contract, central administrative and learning systems (such as virtual learning environments and other educational content) that schools access via the same network connection.<br>In any case the overarching purpose of the school is to enable and improve the quality of the education provided by the school, rather than to provide Internet for its own sake. |
| **Questions for guidance:** | Is the school, the authority or the RBC the "communications provider"?<br><br>Is the school, authority or RBC an "Internet Service Provider", given that the main purpose of the network connection may well be to access the centrally provided administrative and educational services, rather than the Internet?<br><br>If so, who is the "subscriber" since a child cannot form a legal contract? |

## *Group G: Universities and colleges*

| Scenario G16.: University and College access | |
|---|---|
| **Situation:** | Access to the Internet is considered an essential part of research and education. The JANET network that connects all UK Higher and Further Education organisations together and to educational networks elsewhere in the world also provides them with access to the commercial Internet. HE and FE organisations, in turn, provide both JANET and internet access to their students, staff and visiting researchers.<br><br>Universities and colleges 'own' their IP address allocations and may obtain these from ARIN, RIPE or JANET(UK) in its role as a Local Internet Registry (LIR) for RIPE.<br><br>Universities and colleges are required by the JANET Acceptable Use Policy to deal effectively with any reported infringements of copyright; most use a process developed jointly by JANET(UK) and FACT that already contains equivalent duties to the "ISP" role envisaged by the *Digital Economy Act 2010*. |
| **Questions for guidance:** | Is the university or college an "Internet Service Provider" or just a "communications provider", given that the main purpose of their JANET connection is to communicate with other educational organisations, rather than the Internet? |

## *Group H: Prisons*

[Awaiting information]

## *Group I: Oil rigs*

[Awaiting information]

## *Group J: Care homes*

| Scenario J17.: Care homes | |
|---|---|
| **Situation:** | A company provides long-term residential care or assisted living to vulnerable people. E.g. elderly and infirm, respite care, hospice care.<br><br>The persons housed may live in individual dwellings on a campus or within rooms or flats within a single building. They may or may not have their own postal addresses; they do have their own telephones and DSL lines.<br><br>The care provider manages the provision of basic services (power, water, phone service, Internet) to the dwellings. The service providers operate a corporate account for the care provider; the service providers maintain a reference of the property being served to aid the care provider's administration. The billing relationship is between the service provider and the care provider. If it is a private body the care provider may charge a lump sum fee or a menu fee to the person housed; alternatively the facility may be publicly or charitably funded. |
| **Questions for guidance:** | Is the care provider a subscriber or a communications provider?<br><br>If it is a subscriber, should a single tally be made of every complaint received or should individual records be kept?<br><br>Is this scenario objectively distinguishable from the case of an employer who provides home Internet access to its employees? (Scenario B7) |

## *Group K: Hybrid Commercial / Domestic Wireless Hotspots*

| Scenario K18.: Commercial wi-fi hotspot ISP using domestic router | |
|---|---|
| **Situation:** | A commercial ISP provides a domestic consumer with a router that operates a publicly available commercial wi-fi hotspot.<br><br>The domestic customer uses the router for ordinary fixed line Internet access via Ethernet or their own wi-fi connection (SSID). External users see a separate wi-fi SSID that they can access.<br><br>The external end user can obtain Internet access by keying in their credit card details or by entering in an account password previously obtained from the ISP. Access control (RADIUS), branding, the contractual relationship, the billing relationship and routing are all provided by the ISP to the external end user.<br><br>The router is owned by the domestic customer, and to some extent controlled by them (they can, for example, switch it off). Disconnection of the DSL line supplying the router will disable not only the domestic customer but also all external users.[7] |
| **Questions for guidance:** | Is the domestic customer a "communications provider"? |

[7] LINX is reluctant to tie these descriptions to any particular company or product, but for the sake of clarity it is worth making reference to the BT FON product offering (www.btfon.com), which appears to have similar characteristics to those described. We are uncertain as to whether BT FON matches this description exactly, but even if it does not, its existence demonstrates at least the potential for products of the type described.

## *Group L: Landlords for accommodation with services*

| Scenario L19.: Student accommodation with separate services | |
|---|---|
| **Situation:** | A landlord owns a multiple-occupancy building – a block of flats – which it rents e.g. to students. Each apartment has a separate rental agreement [this may be an independent tenancy or, in an alternative case, may be simply a contract for shared use].<br><br>The landlord contracts with an ISP for the provision of Internet access, which is supplied to a router in the building. The building is fully wired for Ethernet, so each student accesses the router and hence the Internet using a fixed connection.<br><br>Before accessing the Internet for the first time students are directed to a self-provisioning portal run by the ISP, where they are asked to identify themselves; however the ISP has no way of verifying their identities and students could well give false details. The self-provisioning portal requires the student to agree to Terms of Use before the Ethernet port is activated for general Internet use; before this is done, only the self-provisioning portal is accessible from that Ethernet port.<br><br>In an alternative case, no such self-provisioning occurs and Internet access is always available. |
| **Questions for guidance:** | Is the student a subscriber?<br><br>Is the landlord a subscriber or a communications provider? [Is it even possible for both the landlord and the student to be the subscriber at the same time?] Is the landlord an Internet Access Provider? i.e. who has the responsibility of sending warning letters (copyright infringement notifications) to the subscriber – the landlord or the ISP?<br><br>Is the ISP required under the Act to operate a self-provisioning portal of the kind described, or is the alternative case permissible even if that makes it impossible for the ISP to issue warning letters? Is the ISP required to obtain verified details of the students' identity? If so, what means are acceptable?<br><br>Is either the landlord or the student under any obligation under the Act to notify the ISP when tenancy of the room changes, so that the ISP may deactivate Internet access until self-provisioning has occurred again? |

| Scenario L20.: Student accommodation with shared services | |
|---|---|
| **Situation:** | A landlord owns a house which is divided into separate accommodation e.g. for students. A domestic wi-fi access point is provided in a communal area which provides Internet access. Each student rents their own room, and has a separate contract with the landlord. Internet access is not billed separately, but rolled into the general cost of rent in each case.<br><br>The wi-fi access point is not capable of recording which student was assigned which IP address and providing that information to the landlord. |
| **Questions for guidance:** | Is the landlord a subscriber or a communications provider? Is the landlord an Internet Access Provider and if so, is he required under the Act to replace his wi-fi access point with one that can identify the students? |

## *Group M: Resellers*

| Scenario M21.: Resellers (own IP range) | |
|---|---|
| **Situation:** | A "wholesale" ISP sells an Internet access product through a non-exclusive resale arrangement with more than one retail reseller.<br><br>The reseller has a contract with the individual or business receiving the Internet access service, and knows their identity.<br><br>The upstream ISP may know the location of the service but not the ultimate customer name. The ISP will likely have a reference number that enables the reseller to identify the customer name, but each customer may have more than one such reference number.<br><br>**The IP addresses may be registered with RIPE in the name of the upstream ISP; there** may or **may not be an indication in the RIPE database that they have been assigned for use by customers of the reseller.** |
| **Questions for guidance:** | |

| Scenario M22.: Resellers (shared IP range) | |
|---|---|
| **Situation:** | A "wholesale" ISP sells an Internet access product through a non-exclusive resale arrangement with more than one retail reseller.<br><br>The reseller has a contract with the individual or business receiving the Internet access service, and knows their identity.<br><br>The upstream ISP may know the location of the service but not the ultimate customer name. The ISP will likely have a reference number that enables the reseller to identify the customer name, but each customer may have more than one such reference number.<br><br>The IP addresses are registered with RIPE in the name of the upstream ISP and are **dynamically assigned to the upstream provider's other wholesale customers** (resellers), and thence to end customers of numerous resellers. |
| **Questions for guidance:** | What status do each of the wholesale ISP, reseller and eventual customer have, from "Internet access provider", "communications provider" and "subscriber"? |

| Scenario M23.: Resellers (multi-layered) | |
|---|---|
| **Situation:** | An ISP provides an Internet access capability to a large intermediary, such as a local authority. The local authority provides access to a range of other access providers (for example, a library, a community centre, some care homes, some residents in local authority housing and some in social run by Housing Associations); in short, many of the cases described in this paper. The IP address range is registered at RIPE with the ISP. No reference is made to the local authority in the RIPE database; alternatively, the local authority is mentioned, but certainly no deeper than that.<br>Access to the network (that is, account authentication) at the organisational/retailer level is controlled by the ISP – that is, the router in the library uses an authentication token such as a password or certificate to gain access to the network, and this token is validated by an access control server operated by the ISP. (This distinguishes the ISP from a pure transit provider). However account provisioning is under the control of the local authority: that is, the local authority provides authentication tokens to the library, the care home etc; the ISP remains entirely ignorant of the identity of these organisations. This means that the most the ISP would ever be capable of doing would be associating the IP address in the CIR with an access authentication certificate.<br><br>Furthermore, the same process may be repeated lower down the chain, e.g. the Housing Association may assign a password to domestic residents, and the identity of these users will not be available to the local authority. |
| **Questions for guidance:** | Is the wholesale ISP in this example an Internet Access Provider within the meaning of the Act, even though it only has wholesale customers? Is the local authority a "communications provider"? If so, on what legal basis is the wholesale ISP required under the Act to pass Copyright Infringement Reports on to the local authority even though it is a communications provider – as opposed it issues Notices?<br><br>Since the local authority in this example does not assign IP addresses from RIPE, can it still be deemed to be an Internet Access Provider under the Act? Is this still true in cases where the local authority does not hold contact records for the subscriber relating to the CIR (i.e. in cases where the local authority's |

customer, such for example the Housing Association, is deemed to be a communications provider rather than a subscriber)? If neither of these aspects are determinative, what exactly are the qualification criteria to be an Internet Access Provider?

If the local authority is deemed to be an Internet Access Provider, does the Act oblige it to act on CIRs that are not addressed to it received from its ISP not from the copyright owner, in other words a person who is not themselves making a complaint? Since the copyright owner complained to the ISP, does the responsibility for issuing the subscriber notification (warning letters) rest solely with the ISP as the recipient of the CIR?

If the local authority is not an Internet Access Provider, on what legal basis (if any) is the local authority required to readdress and resend these reports on to its own customers (or warning letters, depending on whether the operator at the next layer is deemed a communications provider or a subscriber ? (Note that doing so would also require being able to trace the assignee of the access authentication certificate and associate it with the organisation concerned)?

If the local authority is not an Internet Access Provider, on what legal basis (if any) is the local authority required to provide information on the identity of its “customers” to the ISP to enable that ISP to issue notifications (warning letters). Is the local authority permitted to refuse to release that information without adequate contractual guarantees about the subsequent use of that data by the ISP?

Both in the case the local authority where is deemed to be an Internet Access Provider, and in the alternative where it is not, is it permitted to share in cost recovery from copyright holders.

What plans are there to investigate the calculation of costs when spread across multiple parties such as in this case?