

3rd May 2006

Robindhra Mangtani
Competition Group
Ofcom
Riverside House
2A Southwark Bridge Road
London
SE1 9HA

Dear Robindhra

Ofcom consultation on Regulation of VoIP Services

THUS is pleased to respond to Ofcom's consultation on Regulation of VoIP Services dated 22nd February 2006. THUS plc is a leading UK provider of voice, data and Internet services to corporate customers throughout the UK. Headquartered in Scotland, we provide services in every major UK commercial centre, with one of the widest service portfolios available in the market.

THUS plc has recently acquired Legend Communications plc, who are a provider of VoIP services.

Discontinuance of the Interim Forbearance Policy

We are disappointed that Ofcom has chosen to discontinue the Interim Forbearance Policy, as we believe that this policy was in the best interests of both operators and consumers. With the policy in place, operators – particularly VoIP operators – could choose whether to take the benefits of being PATS (for example, number portability) and accept the obligations, or to reject both. As a result, there was an opportunity for diversity in the market.

By discontinuing this policy, those providers who offer services that meet the “gating criteria” are forced to accept the obligations of PATS even if they receive no benefits from them. In some cases these obligations will be onerous and operators will look for ways to escape them. While there may be other approaches¹, an obvious route (perhaps the most obvious) is to withdraw access to 999. As a result, we believe that Ofcom's action will be to reduce the availability of 999 access from such providers with no redeeming benefit to the consumer.

We believe that the consumer protection measures in the consultation are – if enforced properly – sufficient to ensure that new subscribers are aware as to what they are getting in respect of emergency access. It would be better for Ofcom to allow diversity by retaining the Interim Forbearance Policy and finding a sounder legal footing for it.

¹ For example, following the same logic as Ofcom, a service that does not allow outgoing calls to international numbers would not meet the gating criteria.

Detailed Responses to Questions

Question 1: Given recent developments, do you agree that Ofcom's focus should be on the following three objectives in developing our policy for VoIP services, namely (in so far as is possible) (i) enabling innovation in a technological neutral way, (ii) ensuring consumers are well informed, and (iii) ensuring maximum availability of 999 services?

We agree with the first two of these general principles. Innovation should be made possible irrespective of the technical details, and regulation should be carried out in a way that does not unduly advantage one technology over another. Consumers should then be free to choose the service that best suits them; this requires them to be well-informed.

We agree that reliable 999 services are important and should be made as widely available as practical. However, this does not mean that every telecommunications service must be required to provide it. For example, in business premises other arrangements may be made for handling emergencies, and it is only necessary for certain lines to have reliable access to 999. This situation applies today and we see no particular reason to change it.

We believe that it is preferable to allow 999 service to be provided, even if unreliable, rather than produce regulations which have the effect of blocking access to 999 because the provider cannot meet some arbitrary other standard that has been tied to 999 provision. Similarly, while location information is useful to the emergency services, we would not want to see a regulatory regime where providers would find themselves pushed towards blocking access to 999 because they are unable to provide reliable location information. An indication of an unreliable location such as a main business address, properly marked as such, when 999 is available is of greater value than having no access to emergency services at all.

We do not agree with the suggestion in paragraph 3.7 that consumers will deliberately choose services without 999 access on the assumption that they will be able to use other facilities if the need arises. Does Ofcom have any evidence from consumer research that supports this view?

Question 2: Do respondents agree with this approach for the interaction between network providers and PATS providers?

We believe that any PATS obligations should lie entirely on the PATS provider. Where the service is carried over an ECN operated by another provider, the PATS provider should use contractual agreements to ensure their obligations can be met; these, and any enforcement actions related to them, should remain on the PATS provider and not the ECN provider. Rather than requiring network providers to show that GC3 should not be applied, it should be for Ofcom to identify who is the PATS provider and enforce the requirements on them (in effect, an "innocent until proven guilty" approach rather than the opposite).

Question 3: Do you agree that the limitation of GC 3 obligation to providers of service at a "fixed location" is not sustainable in the long term? What views do you have on how this may be addressed?

The widespread introduction of centralised intelligence in telephone networks (e.g. SIP based call servers) rather than distributed decision-making in call switches means that nomadic service (even if only on an occasional basis) will become more common in the future. This means that we agree that the term "fixed location" is not sustainable in the long term or even the medium term.

We note that any telephone number served by such a network is, technically, not a “geographic number” even if it is always provided at a single location, because the number does not contain any component with “geographic significance used for routing calls to the physical location of the network termination point”, contrary to the definition in the Universal Service Directive. Therefore all numbers on Next Generation Networks are “non-geographic numbers” for the purposes of the Directives, no matter what users may think. This may or may not help in resolving the issue.

We suggest that the General Conditions need to be revamped to address the distinctions between network and service and between number, NTP, and service. This may require a similar revamp of the relevant Directives; however politically difficult this might appear to be, though the 2006 Review provides a timely window of opportunity, any other approach will merely patch the problems temporarily but make them worse in the long term.

Question 4: In light of the other measures proposed in this document, are there particular issues in relation to VOIP services that should be addressed in this review?

Though it is not directly related to this review, there are a number of issues related to numbering that VoIP brings into sharper relief. For example, we find that customers want geographic numbers, not so much to indicate their location, but because they are familiar with them and understand them as being cheap (or free, with many calling plans) to call. An “indeterminate location” geographic number range with these properties (which 056 very definitely is not) would be worth considering, provided that there are strict controls in place to ensure that it retains the same properties as “true” geographic numbers and is not subject to discriminatory charging. We will be addressing this point further in our response to the Numbering consultation.

Ofcom should also be looking at ways to encourage direct interconnection between VoIP carriers.

Question 5: Are there particular issues in relation to VoIP services that should be addressed in this review?

See our response to question 3.

Question 6: Do you have any comments on Ofcom’s proposed modification to the PATS definition in GC 18?

We have no objection to the proposed modification, since it brings the wording into better harmonization with Article 30 of the USD.

It is our interpretation of Article 30 that portability only applies where both the donor and recipient service providers are providing PATS. Specifically, the requirement in 30.1 is to allow any undertaking to provide the service – a publicly available telephone service – and not to allow any undertaking to provide *any* service. This means that the obligations to provide Portability only apply when the recipient is a PATS provider, as suggested by paragraph 5.32 and contrary to the implications of paragraph 5.5. We would recommend that Ofcom clarify this in GC18.

Notwithstanding the above, we disagree with the policy approach of using number portability as a “carrot” to encourage 999 access. There are many situations where such access is not an essential part of the service to be provided (e.g. many business services) and adding the arbitrary requirement for PATS before allowing portability will discourage innovation in such services.

Question 7: Do you agree with the proposed application of the code?

Yes. However, the code should apply to all telephone services, irrespective of the technology used to deliver them.

We have, however, identified a possible lacuna in the Code. If an operator wishes to change the service provided (e.g. by no longer providing a directory) there appears to be no specific requirement to apply the requirements of the code. While normal consumer legislation will apply, "Change of Service" should be a further situation mentioned by the Code, in a similar way to "Sales Process" or "Point of Signature".

Question 8: Do you agree with the proposed approach for informing consumers that services may cease to function if the broadband connection fails or there is a power cut or failure?

Yes. However, the message should be more specific (for example, it is not clear whether it refers to a power cut at the subscriber's location or elsewhere).

Question 9: Do you agree with the proposed approach for informing customers where access to emergency calls is not available?

We are generally in agreement. However, it is not clear that all VoIP systems will be able to provide a recording of the type described when 999/112 is dialled, and the option of simple NU tone should be retained.

Question 10: Do you agree with the proposed approach for informing consumers that access to emergency calls may cease to function if the Data Network fails or there is a power cut/failure?

Yes.

Question 11: Should the code be extended to point of signature acknowledgement in respect of reliability of access to emergency calls?

Yes.

Question 12: Do you agree with the proposed approach to location information providers where the service does provide access to emergency calls? In particular, do you believe that subscribers should be required to register their main location prior to activation of the service?

We generally agree with this approach. However, users should not be prevented from using the service if they have not provided a location. There are scenarios where this would be onerous, and it will simply encourage users to provide an incorrect address (for example, by stating that they are still at their previous location) in order to get round the restriction. Indeed, it may well be the case that the user either does not know their correct address (if sitting in a café or a hotel room, the correct street address may well not be obvious) or they are at a location that doesn't have an address (WiMAX services will make it practical to use VoIP from the middle of a forest).

Question 13: Do you agree with the proposed approach to informing consumers where services do not provide emergency location information?

Yes.

Question 14: Do you agree with the proposed approach to informing customers where services do not provide number portability?

Yes.

Question 15: Do you agree with the proposed approach to informing consumers about the types of facilities that might not be available, but which they have come to expect from a telephone service?

We are not clear that all of the services listed are “standard” on existing lines² and would be expected by consumers. If VoIP providers are to be required to make it clear that these are not available, then so should “traditional” telephony providers, including mobiles.

Question 16: Do you agree with Ofcom’s view that all aspects of the code of practice should be mandatory?

We believe that the code should be made mandatory on all telephony service providers.

Question 17: Do you consider that the overall programme of activities is appropriate?

We do not have any issues with the overall programme proposed, but would not wish to see further regulation without public consultation on a wide scale.

Question 18: In light of Ofcom’s Consumer Policy Review, are there other consumer education measures that Ofcom should consider?

We do not have anything to suggest.

Question 19: Do you have comments on this proposed enforcement approach?

No, provided that it is applied equally to all telephone providers, both traditional fixed line, mobile, and VoIP.

Question 20: Are there other areas of research activity that Ofcom should consider to ensure it understands market developments?

We do not have anything to suggest.

Question 21: In relation to ensuring high availability of 999 access, are there other measures that Ofcom could consider?

We do not have anything to suggest.

Question 22: Do you agree with Ofcom’s approach to naked DSL?

No. Firstly, we consider that naked DSL usefully fills a gap between unbundled local loops on the one hand (requiring a physical presence at the exchange) and Wholesale Line Rental on the other. All the concerns expressed concerning reliable emergency services access already apply with the former, since there is no requirement to use these loops for a PATS service.

Even if naked DSL was prohibited or restricted to PATS providers, this does not mean a useful PSTN service would result. For example, where a subscriber has chosen to use VoIP because of reduced call costs, they may well not plug a telephone handset into the PSTN

² We can provide examples in confidence.

line, effectively using it as if it were naked DSL and connecting the various sockets in the house to the VoIP adaptor.³

Question 23: Do you agree a cross industry meeting would be a useful approach to move this issue forward? What other steps could be taken to provide support for 056 numbers?

We are not convinced that consumers see the benefit in 056 numbers. Because pricing of these numbers is not tied to geographic call rates, we believe that they are likely to be seen by most consumers as expensive to call, like 0870 or 070 numbers, and therefore undesirable. Similarly, even if the datafill issue can be resolved, we query how many foreign operators allow calls to these numbers. Again, we will be addressing this point further in our response to the Numbering consultation.

Question 24: How can a VoIP call be traced for detection and prevention of malicious and nuisance calls? How could a suitable call screening service work in a VoIP network?

Tracing a VoIP call requires the retention of SIP registration logs as well as call logs themselves. It is not clear what the legal situation is with respect to such retention (is it required by the Data Retention Directive, forbidden by the Privacy Directive, or even both?). Ofcom needs to investigate and clarify this matter.

Where VoIP calls are made through a carrier, call screening should be easy in principle, since there will be a verified identity for the caller (even if this is not an E164 number, it can be used in the same way as CLID). Where calls are made directly between end-points, however, it will be much more difficult to trace callers. Intermediate CPs will not have the ability to screen calls without major changes to their networks, changes that would be ill-advised for other reasons.

Question 25: Do you agree that SPIT could be a potential problem and what techniques can be used to minimise the impact of SPIT on consumers of VoIP services.

We do not believe there is a significant threat from SPIT in the near future. At present the overheads required to set up a SPIT campaign are far greater than those required for email spamming, with far less return. By the time that SPIT becomes economically viable, we expect counter-measures to be available and generally used.

Question 26: Have there been any instances of a VoIP service being compromised or used to deliver malware or a DoS attack?

We are not aware of any instances of this.

The question appears to be based on a misunderstanding of malware and how it operates. It is not the case that anything transmitted over IP or the Internet is automatically a route for delivering malware, any more than it is the case that the TDM telephone network is immune from it. Data is data; it can only become “malware” if the receiving application provides a way to interpret it as such. For example, the G.711 encoded voice packets used in VoIP could have their payload replaced by malware, by MP3 encoded music, or even by the PDF file comprising this consultation, but the receiving system is going to continue to treat the data as G.711 and convert it to a (probably noise-like) sound. It will not be looking to see if the voice data “looks like” something else and treat it differently. Note that GSM phones already process packets in just this way, yet voice calls cannot be used to distribute malware. There is only a problem if the receiving device has a mechanism to take the data and re-interpret it as commands.

³ Anyone with teenage children will understand the reasoning here.

For example, email viruses aren't a problem because of email, they are a problem because certain email software will take certain forms of data and treat it as instructions to be carried out – these instructions can examine the address book and send out emails without the user's knowledge. It is this bad design decision that allows malware distribution. Unless VoIP phones are going to (say) start listening for embedded DTMF tones and interpret them as instructions to make outgoing calls without the user's permission, there isn't going to be a problem.

Note that, while there is a malware issue with mobile phones, it is not caused by the use of packetised voice data. Rather, it occurs because modern handsets have the ability to receive and execute application programs (games, electronic wallets, currency conversion tools, and so forth).

The major fraud issues with VoIP at present are ones that apply equally to traditional telephony: stolen credit cards used to sign up for services that are then abused, or customer log-in details being compromised and the perpetrator then making free – to them – calls using these details.⁴

As for DoS attacks, while they are no doubt possible, the issues and defences are the same as with any Internet-based service.

Question 27: Are there any other considerations that need to be taken into account when a provider does not have a UK entity?

We are unable to suggest any.

Question 28: Is it reasonable to ask VoIP service providers to participate in schemes designed for e-commerce?

No. VoIP providers will use mechanisms like SSL if they are beneficial, but the technical issues⁵ and different social network⁶ mean that techniques and schemes from e-commerce may not be suitable for VoIP. Any requirement on providers should be limited to requiring them to publish information about security and privacy (e.g. under regulation 5 of the Privacy and Electronic Communications (EC Directive) Regulations 2003⁷, and to publish the details of the data protocols and encryption algorithms used (e.g. as required by regulation 13 of the Radio Equipment and Telecommunications Terminal Equipment Regulations 2000)⁸.

Question 29: Do you have any other comments on the proposed approach to investigating the application of the GCs applicable to providers of PATS in the context of VoIP?

No.

Question 30: Do you have any comments on Ofcom's views on the meaning of above mentioned terms and legal concepts?

⁴ The traditional equivalent of these details are the number and PIN for pre-payment or account cards.

⁵ For example, e-commerce systems are usually using HTTP over TCP/IP, which provides a reliable delivery of every single byte of data, while VoIP will probably use RTP over UDP/IP, which does not attempt to re-send corrupted or lost packets – it is better to have a “click” or a few milliseconds of silence than to introduce the end-to-end delays that TCP would introduce. Reliable delivery is essential for SSL to work, and so it cannot be used over UDP. Other encryption schemes which do not have this problem are available, such as IPsec.

⁶ E-commerce involves a large number of consumers dealing with a relatively small number of businesses who can afford to put some effort into setting up their systems. Telephony involves consumers calling one another, and so cannot rely on mechanisms that require more than a trivial effort to set up.

⁷ S.I.2003 number 2426.

⁸ S.I.2000 number 730, as amended by S.I.2003 number 1903.

While we agree with the interpretation of “fixed”, see our response to question 3 for our opinions on the long-term viability of this approach.

Question 31: Are there any other steps that a VoIP service provider could consider in respect of the IP network layer and service application layers to ensure network integrity?

We do not have any comments to make.

Question 32: Are there any other steps that a VoIP service provider could consider in respect of parts of the underlying network that they do not control?

We do not have any comments to make.

Question 33: What additional steps could a VoIP service provider take to support nomadic users with regard to maintaining network integrity?

We do not have any comments to make.

Question 34: Do respondents consider whether other options to ensure continuity in the case of a power outage are appropriate?

We do not consider that continuity in the case of a power outage should be a responsibility of the service provider, provided that the customer has been made aware of the issues. Provision of continuity could, of course, be a positive selling point.

Question 35: What other steps could be taken to provide reliable location to assist the emergency services in their work?

We are involved in the work described in 2.14 and A6.88. However, this is a “hard” problem for a number of reasons (such as those described in this section) and we do not believe that a satisfactory “100%” solution is even on the horizon. In particular, we do not agree that any of the suggestions in this section form an acceptable solution, particularly for nomadic users. Hopefully future research and development will produce something.

Question 36: What other steps could be taken to provide reliable location to assist the emergency services in their work in the case of nomadic users?

The answer to question 35 applies here as well.

Question 37: In addition to participating in the NICC working group on providing location in IP networks and the 112 expert group, what other steps should Ofcom take?

Ofcom could commission technical research and development in this area.

Yours sincerely

Clive Feather
Regulation & Interconnect Department

Cover sheet for response to an Ofcom consultation

BASIC DETAILS

Consultation title: Regulation of VoIP services

To (Ofcom contact): Robindhra Mangtani

Name of respondent: Clive Feather

Representing (self or organisation/s): THUS plc

Address (if not received by email):

CONFIDENTIALITY

What do you want Ofcom to keep confidential?

- | | | | |
|----------------------|-------------------------------------|---|--------------------------|
| Nothing | <input checked="" type="checkbox"/> | Name/address/contact details/job title | <input type="checkbox"/> |
| Whole response | <input type="checkbox"/> | Organisation | <input type="checkbox"/> |
| Part of the response | <input type="checkbox"/> | If there is no separate annex, which parts? | |

Note that Ofcom may still refer to the contents of responses in general terms, without disclosing specific information that is confidential. Ofcom also reserves its powers to disclose any information it receives where this is required to carry out its functions. Ofcom will exercise due regard to the confidentiality of information supplied.

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response. It can be published in full on Ofcom's website, unless otherwise specified on this cover sheet, and I authorise Ofcom to make use of the information in this response to meet its legal requirements. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Clive Feather

Signed (if hard copy)