BEREC Call for Contributions on Possible Existing Legal and Administrative Barriers with Reference to the Provision of Electronic Communications Services for the Business Segment – Joint Response By:

AT&T, BT Global Services, Cable & Wireless Worldwide, Orange Business Services and Verizon Business

Introduction

This response is submitted on behalf of the following companies: AT&T, BT Global Services, Cable & Wireless Worldwide, Orange Business Services and Verizon Business. We applaud BEREC for initiating this proceeding and recommend that the issue of administrative barriers continues to form part of BEREC's activities for the remainder of 2011 and into the 2012 Work Programme.

All our companies are engaged in the provision of pan-European and global services to large enterprise customers, and have legal entities in several EU Member States. The high-end, large business (enterprise-level) services that we provide are differentiated from mass-market consumer services in a number of key respects, and typically involve the following attributes:

- Significantly more complex telecom services are provided, comprising multiple locations across countries, different access technologies, bundles of services, and very demanding Service Level Agreements (SLAs).
- Sophisticated knowledge of the technology and economic implications of telecommunications services among high-end business users.
- Comparatively small numbers of total customers.
- Extensive bi-lateral, individually negotiated and tailored contracts.
- Professional use of the services provided.
- Products that are different to those used by consumers, and that typically run mainly on private IP networks, distinct from the public Internet, and involve a high degree of traffic management to meet customers' demands and requirements.

Answers to BEREC's Questions

1) ***Under the current authorisation regime laid down by the 2002 Authorisation Directive (and substantially confirmed by the 2009 review), the ECNS operators are entitled to start activities upon notification/declaration to the NRA.***
   - ***What is your overall experience of the practical implementation of such administrative regime in member States?***
   - ***Did you encounter inconsistencies or operational constraints potentially affecting the provision of cross-border business services? If yes, please provide a description.***

Under the Authorisation Directive, notifications must not entail more than a declaration by the provider of the intention to commence service or operations, and "minimal information which is required to allow the national regulatory authority to keep a register." In practice,

notification requirements vary significantly between Member States as regards the categories of networks and services that may be declared. Some Member States have extensive categories of potential networks and services to be notified. The result of this variation in notification approaches is that provision of identical services across the EU Member States will be registered in quite different categories in each Member State. This in turn means that different regulatory treatment and obligations apply to the same services. Not only does this variance create complexity for service providers, it must impede the ability for Member States to compare information about their markets.

Furthermore, very few National Regulatory Authorities (NRAs) facilitate the online filing of notifications, while offline notification processes can be very cumbersome, sometimes requiring the (re-)submission of company registration documentation and corporate information each time a new product service is launched that falls within a notification category that has not been previously declared. A recent study[1] for ARCEP by Hogan Lovells and Analysys Mason noted that:

> "The principal difficulty for operators, however, arises from the obligation that they are supposed in theory to keep ARCEP informed of any change to the information provided at the time of the initial declaration. This is an obligation that they do not necessarily satisfy in practice. Similarly, it can happen that operators omit to inform ARCEP of the withdrawal of service of network operation activities when this occurs." *(Our translation from the original French)*

The study for ARCEP also highlights that operators' rights and obligations exist independently of whether a declaration has been made:

> "In theory, the status of electronic communications operator and the rights and obligations that go with it exist independently from any declaration by virtue of the very activity of the entity in question. Not having notified its activities to ARCEP does not therefore exonerate an operator from its other obligations. BNetzA and OPTA share this analysis." *(Our translation)*

We believe that unnecessary complexity would be removed if regular renewals of notifications were not mandated (as they are in Italy, for example) and updates to notified network and service categories were left to the discretion of business service providers.

2) ***As far as the administrative regime is concerned, can you identify some national best practice across Europe which may help in supporting the provision of cross-border business services?***

We note that the UK and Denmark have chosen not to implement a notification requirement as part of their implementation of the EU authorisation regime, and that the regulators in these countries do not appear to confront any difficulties in regulating markets. We would therefore encourage BEREC to explore the scope for more regulators to abolish notification

[1] *Étude sur le périmètre de la notion d'opérateur de communications électroniques*, Étude réalisée par Hogan Lovells et Analysys Mason pour le compte de l'ARCEP, June 2011

requirements. Where this is not considered feasible, a simplified notification arrangement should be adopted with a minimal number of categories and scope for notifying providers to submit "free hand" descriptions of services which do not fall within any standard categories. We would strongly urge regulators to develop a common, consistent format for notifications that would be used by all regulators not in a position to abolish notifications completely.

In some Member States, for example, in Austria, Finland and Romania, it is possible to make notifications/declarations online. In our view, this should be possible in every country applying a notification obligation and such an improvement would be consistent with efforts by institutions across the European Union to move more administrative processes to the online world.

We would also encourage regulators to make notifications possible in other EU official languages, or, as a minimum, to publish information about notification regimes in one or two of the principal official languages of the EU.

3) *Besides the authorisation system, are there any other differences in administrative procedures in the area of telecommunications that may affect the provision of business services across Europe?*

We believe there are a number of administrative obligations which limit the provision of uniform business services across the European Union. We acknowledge that not all the matters described below will fall within the competences of the NRAs represented in BEREC, but we consider it important to provide a complete picture of the inter-related areas. We would regard items A to E below to be priority areas for attention by BEREC.

A. Reporting Obligations

Description of Issue: NRAs require electronic communications network and service providers to complete multiple financial, statistical and market analysis reports. There is little consistency in the format or data categories of these requests, and there are significant variations in practice. All of this adds cost and complexity of providing cross-border services. Not only does this variance create complexity and additional administrative burden for service providers, it must impede the ability for Member States, BEREC and European Commission to compare information about their markets.

Recommendations

1. Develop common forms and approaches for the reporting of financial, statistical, service category and other market information by electronic communications networks and service providers.

B. Administrative fees

Description of Issue: Administrative charges are levied in most Member States and are mostly related to revenue from electronic communications, although some NRAs apply a

flat fixed fee (e.g., France), a variable fee with a high minimum payment (e.g., GBP 55,000 in Gibraltar), or fees related to the type of service provided (e.g. Belgium, and the Ministry of Communications' fee in Italy). High fixed flat fees can be a barrier to cross-border business service providers with relatively low revenues compared to the major national players.

Where revenue-based fees are applied, the calculation of such charges varies significantly. Some NRAs require fees to be based on total electronic communication service revenues, while others apply a 'net revenue' or 'value added' approach (with fees based on revenue after deduction, respectively, of telecom or total costs).

The evidence required to certify accuracy of declared revenue (where this is the charging basis) also varies significantly between Member States. In some Member States, providers are required to submit audited financial statements, or auditable accounting methodologies. In several Member States, however, it is possible to self-certify revenue without the need to provide audited financial information.

Recommendation

1. Adopt a common revenue-based system for the calculation of the fee with self-certification of revenue. (In all cases, fees should be strictly reflective of the true costs of regulating the market and should be linked to cost-efficiency objectives to be met by NRAs.)

C. Inappropriate Application of Consumer Protection Obligations to Business Service Providers

Description of Issue: A number of NRAs seek to impose consumer protection obligations which have little relevance or applicability to larger enterprise customers, for example, requirements regarding publication of prices, terms and conditions, as well as consumer codes of practice or service charters, availability of consumer complaint-handling procedures, alternative dispute resolution schemes, compensation arrangements and termination of service. It is difficult to see the relevance of these obligations in the context, for example, of heavily negotiated contracts that follow competitive tendering processes with large enterprise customers.

In the case of cross-border providers of business communications services, these contracts are for multi-country solutions and the arrangements for such matters are not specific to any country or geography. Furthermore, the contracts are usually negotiated with the full involvement of the legal services of both the supplier and customer, so the concerns behind such consumer protection requirements do not arise, or are specifically managed in the contract. It is a different circumstance from mass market consumer services.

Recommendations

1. Apply a common, pragmatic and flexible approach to the application of consumer protection obligations, either by de jure or de facto exempting business services from these requirements.
2. Analyse the harmonisation of obligations on emergency calls in the context of VOIP.

3. Impose longer implementation terms for number portability in case of business providers with multi-site clients where migration is more complex than the portability of the number of a single user.

D. Net Neutrality

Description of issue: With specific regard to the new the newly adopted "net neutrality" provisions in the Citizens' Rights Directive (increased meaningful transparency, NRAs' authority to set minimum Quality of Service (QoS) if needed), these were clearly intended to improve consumer protection through increased awareness and choice. The needs of consumers (i.e., residential users) and large business customers in relation to Internet access differ considerably. In particular, the asymmetry of information that may exist in the consumer context does not arise in the case of contracts that are heavily negotiated with informed enterprise customers following competitive tendering processes. Therefore, regardless of whether increased meaningful transparency rules and possible minimum QoS levels are appropriate in the consumer protection context, we believe Member States and NRAs should not automatically apply the same provisions to large business users.

Recommendations

1. Exclude business services from transparency and Quality of Service obligations (minimum standards, publications, etc.)

E. Quality of Service Reporting

Description of Issue: NRAs have a legitimate interest in ensuring consumers have access to relevant, comparative, QoS information to allow them to determine the right service provider to meet their needs. If regulatory intervention is determined to be necessary in relation to QoS reporting and publication requirements, we believe that high-end business customers should be excluded from any such regulatory scheme. Large enterprise customers have sufficient buying power to negotiate and demand service levels to meet their needs. Accordingly, any imposition of a QoS reporting scheme for large business service providers is unnecessary and would not, in our view, meet the tests of being justifiable or proportionate.

Ofcom's decision in August 2009[2] to repeal its so-called Topcomm Direction of 2005 provides a salutary lesson in the pitfalls of ill-conceived regulation in this area. The Topcomm Direction had required fixed line voice providers to capture and publish comparable information on specific aspects of QoS (e.g., installation, fault rates, fault repair, complaints-handling) for consumers and business users. In withdrawing the regulation, Ofcom noted a widespread consensus from stakeholders that the Topcomm scheme was not fit for purpose, as well as the low usage of the comparison website and the scheme's high running costs. Ofcom also cited views from several business service providers that the Topcomm scheme was particularly ineffectual and burdensome to them,

[2] *Topcomm Review: Quality of Customer Service Review*, Ofcom Statement, 29 July 2009, available at: http://stakeholders.ofcom.org.uk/consultations/topcomm/statement/

as business customers, particularly large corporate clients, do not find such information useful and are more likely to negotiate their own individual service level agreements. Since withdrawing the QoS reporting Direction in 2009, Ofcom has not sought to impose any replacement scheme on business service providers.

Recommendations

1. Exclude business services from comparative Quality of Service reporting and publication obligations.

F. Legal Establishment

Description of Issue: It is often not possible for a company established in one Member State to register directly under the notification regime of a neighbouring Member State. Business service providers are frequently obliged to establish local legal entities or branches in each Member State of operation, even if they have no local employees or any physical infrastructure, other than perhaps a network node housed in a third party telehouse. This barrier to entry and cross-border service provision sometimes arises explicitly in the authorisation regime of certain Member States, whereas in other instances it is a result of restrictions in company law, tax or other parts of the legal framework.

Recommendations

1. As a minimum, Member States and NRAs should ensure that there is nothing within the terms of their electronic communications authorisation regimes that would prevent a company established in one Member State from operating under the authorisation regime of any other Member State without the need to create local subsidiaries or branches.

G. Network Security Obligations

Description of Issue: New obligations on security and data breaches have been introduced in Article 13 of the revised Framework Directive. Such obligations foresee national guidelines on network security and availability, reporting obligations and audits that operators must pay for. We note that work is under way within ENISA to develop a common approach to the implementation of the security elements of the new obligations across Member States, with particular regard to establishing minimum standards, as well as reporting templates, metrics and thresholds. We are pleased by the recognition of the importance of a consistent approach across European countries. This will minimise the extent to which pan-European business service providers need to adopt a different approach in each country and ensure providers in one country do not incur a greater regulatory burden than in others.

The situation that all stakeholders (not just industry) should be anxious to avoid is one where Member States each come up with their own guidelines which differ or go beyond those ultimately issued centrally. This unfortunately appears to be a real possibility given that Article 13(4) goes on to say "[Measures adopted by the Commission] shall not prevent Member States from adopting additional requirements [..]."

It should also be recognised that large business providers are often global in nature, and will have systems and processes that reflect this. Any obligations arising in the EU should incorporate sufficient flexibility to allow compliance to be demonstrated in ways other certification against specific EU or national standards.

A further benefit will arise if Member States can generate and submit the required reports to the Commission and ENISA using a consistent approach. However, if the clear benefits of having a co-ordinated approach across Europe are not delivered by this process, then the European Commission should consider using its powers under the new regulatory framework to introduce technical harmonising measures.

Recommendations

1. Member States and NRAs are strongly encouraged to NOT go beyond the guidance or measures adopted by the Commission/ENISA. A fully harmonised approach is of key importance.

H. Personal Data Breach Notification

Description of Issue: Article 4 of the revised e-Privacy Directive requires providers to notify personal data breaches to the competent national authority. It also requires that "[w]hen the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach [..]." Article 4(5) also gives the Commission the power to adopt implementing measures to ensure consistency. We note that the Commission has recently issued a consultation on this issue.

The key point is that large business providers are not in the same position as those operators offering services to consumers. Large business providers are engaged with business clients, which raises the question whether they handle personal data at all. Interpretations differ across Europe. In any case, business providers are typically at least one step removed from the final end user and are unable to identify individual end users from the traffic carried. This means that, in the vast majority of cases, it would not be possible to provide meaningful notifications to authorities or to notify the subscriber(s) concerned. As a result, business providers would expect to be responsible for only a tiny fraction of notifications, if any. This should be recognised both by the Commission and also competent national authorities.

Recommendations:

1. Provide a harmonised answer to the question whether business providers handle any personal data and fall in scope of this new requirement. To the extent that business providers are covered by such notification requirements, it is imperative that measures are consistent, simple, and take account of providers that make very few notifications.

I. Lawful Intercept

Description of Issue: Nearly every country requires communications service providers (CSPs) to cooperate with investigations by law enforcement agencies (LEAs), including with LEA requests for lawful intercept (LI) of communications. Until recently, such obligations imposed specific requirements to build network capabilities to support LI only on a small number of infrastructure operators and mass market voice service providers. Now, driven by the ongoing migration to Internet Protocol (IP)-based services, many countries are adopting and implementing requirements, including on business service providers, to build network capabilities that support LI at the demand of LEAs. Such broad LI mandates on business service providers can impose significant costs, technological challenges and regulatory uncertainty (including by using existing inadequate LI technical standards).

In a recent paper[3] on this issue, the International Chamber of Commerce (ICC) makes several recommendations for providing LEAs with all or most LI capabilities that they reasonably require, while minimising unnecessary adverse effects on market players. In particular, Recommendation 2 states that CSPs serving only enterprise customers should be subject to minimal, proportionate LI capability obligation, while Recommendation 3 calls for proportionately lighter regulatory obligations to apply to small CSPs with few customers in a given country, to keep benefits and costs in balance. The ICC cites examples of best practice in this regard by a number EU Member States. Furthermore, Recommendation 5 of the ICC paper states that centralised, multi-country LI solutions should be permitted, and individual countries should not unreasonably restrict CSPs from meeting LI obligations of multiple countries via centralised facilities, at locations selected based on commercial considerations.

Recommendation

1. The relevant authorities in EU Member States should take full account of the recommendations in the ICC paper.

J. Data Retention

Description of Issue: Data retention obligation defined in Directive 2006/24/EC are not applied consistently or proportionately across the EU. Large business service providers will typically have a relatively small number of customers, compared to mass-market providers, and these customers are far less frequently the subject of serious crime investigations. As a consequence, the number of requests for access to retained data received by business providers is extremely limited, even non-existent for some operators in some jurisdictions. Furthermore, the area of interest to law enforcement is often not available on our servers or network, but rather resides in the domain of the customer who (unlike consumer end users) mostly have their own PABXs or servers that handle the traffic.

[3] *Global business recommendations and best practices for lawful intercept requirements*, International Chamber of Commerce, Document No. 373-492 (June 2010) available at: http://iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/373492LawfulInterceptPolicyStatementJune2010final.pdf

The costs of implementing data retention, which are not recoverable from governments in most Member States, therefore represent a disproportionate burden on this category of provider. These issues need to be resolved in the current review of the Data Retention Directive, but can also be addressed by a more pragmatic implementation and application of the Directive as it stands today.

Recommendations

1. Member States should consistently apply the Directive and never exceed the requirements of the Directive. In-country storage requirements for retained data should not be permitted.
2. The Directive should be applied in a proportionate manner, with consideration given to setting thresholds for when providers must implement capabilities (as is the case in the UK and Finland) or blanket exemptions for (categories of) business service providers.
3. Cost recovery mechanisms should apply to both set up and operation of retention capabilities, and take account of the specificities of business service providers receiving few or no access requests.

K. Measures to Combat Illegal Content

Description of Issue: Member States are increasingly imposing obligations on operators to assist in the fight against illegal content, notably through "graduated response" processes and processes to block access to illegal content (content infringing IP rights, child porn, etc.). Such obligations pose significant technical challenges that are not proportionate to impose on operators with a limited client base, especially when most large business customers apply company usage policies that prohibit downloading or sharing of illegal content. There are also particular challenges for Business ISPs to identify and directly notify the specific alleged infringing end user on the business customer's network.

In the UK, Ofcom has proposed that a Code of Practice to underpin the initial obligations to reduce online copyright infringement (as imposed on Internet service providers (ISPs) by the Digital Economy Act 2010) will initially cover only fixed-line ISPs with over 400,000 subscribers.[4]

Recommendation

1. Limit obligations on measure to combat illegal content to consumer providers or to providers with a significant number of clients. "Significant" will vary by market, but the Ofcom approach is a helpful benchmark.

L. Taxes

Description of Issue: We have observed a tendency from some EU governments to apply taxes to electronic communications services at higher levels than for other services. We

[4] See: *Online Infringement of Copyright and the Digital Economy Act 2010 - Draft Initial Obligations Code*, Ofcom Consultation, 28 May 2010.

endorse the concerns raised by the International Chamber of Commerce in their recent paper[5] on this issue. Such burdensome and discriminatory taxes deter the adoption and use of services that are major drivers of development. The Commission has already addressed new taxes imposed on the industry by the public authorities in France, Spain and Hungary. With particular regard to the calculation and collection of taxes imposed by local governments for the use of public domain for the installation of telecom networks, there is a lack of consistency in some Member States. For example, in Spain and Portugal such infrastructure taxes are even required to be paid by service providers with no infrastructures on the relevant territory. In Spain, there is a requirement to identify revenue earned in up to 8000 local municipalities in order to calculate any due taxes, which are frequently less than the costs of processing the payments.

Recommendations

1. Limit such taxes to operators with installed infrastructure within the relevant territory.
2. Exempt operators with revenues within the territory below a certain threshold.

4) *Do you believe that the provision of cross-border business services could be subject to a specific administrative regime?*

- ***If so, for which reasons and under which legal basis?***
- ***What should be the special features of such regime?***

While we would ideally like to see the emergence of a single pan-European authorisation regime for cross-border business services with only one notification to be made in order to offer such services anywhere in the EU, we do not think there is a legal basis for such a concept at this stage. Nevertheless, this should be seen as the ultimate, long-term objective if a genuine Single Market for business services id to be achieved.

Meanwhile, we do see scope and a basis for gradual, measured improvements to the current situation. The revised EU Regulatory Framework includes an amendment to the Authorisation Directive by way of an addition to Article 3(2):

> *"Undertakings providing cross-border electronic communications services to undertakings located in several Member States shall not be required to submit more than one notification per Member State concerned."*

We believe that this amendment provides grounds for reform to remove some of the current complexities of providing cross-border business services.

Part of the solution could be to introduce a cross-border business service provider category in all national notification regimes. Being able to identify business activity and customer focus

[5] *ICC discussion paper on the adverse effects of discriminatory taxes on telecommunications services*, International Chamber of Commerce, Document No. 373/495 – (26 October 2010) available at: http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/ICC_DiscussionPaper_TelecomTaxes_26Oct10.pdf

in this way could assist NRAs in not imposing unnecessary and inappropriate obligations on pan-European business service providers.

Another solution could be to develop a one-stop shop arrangement whereby cross-border business service providers could make a single notification to one NRA, which would then be automatically replicated by other NRAs specified by the provider. The approach adopted for authorisation of Mobile Satellite Services might provide a template for such an arrangement.

Finally, as previously mentioned, Member States and NRAs should ensure that cross-border provision of services within the EU, without the need for establishment of local legal entities or branches, should be explicitly permitted by national authorisation regimes (even if other, non-telecom related, legal requirements impose such restrictions.

19 August 2011