Report for ComReg

Review of the regulatory framework for VoIP in Ireland

26 October 2010

Ref: 17530-386

analysys mason

analysys mason

Contents

analysys mason

Analysys Mason Limited
Suite 242
The Capel Building
Mary's Abbey
Dublin 7
Ireland
Tel: +353 1 602 4755
Fax: +353 1 602 4777
dublin@analysysmason.com
www.analysysmason.com
Registered in Ireland IR304061

1 Executive summary

The regulatory treatment of VoIP has a complex history. Relevant ComReg documents include:

- A series of decisions related to VoIP services (04/103). These decisions primarily concerned the allocation of numbers to VoIP providers including the opening of a new number range 076.
- Non-binding guidelines for VoIP service providers on the treatment of consumers (Doc 05/50)
- a review of the VoIP regulatory framework (06/45).

Since that time, in 2009, the European Commission has updated the regulatory framework in a number of ways.

In this context, ComReg has commissioned Analysys Mason to conduct a review of the regulation of Voice over Internet Protocol (VoIP) / Voice over Broadband (VoB) in Ireland. Our review has accounted for national developments, as informed by a series of interviews with key stakeholders in Ireland, and the activities of national regulatory authorities (NRAs) across a number of other Member States.

The revisions to the framework cover a number of areas which have specific impact on service providers using VoIP technologies, which we have looked at in turn:

- the security and integrity of networks and services
- access to emergency services, including the ability to make emergency calls, the provision of caller location information, and the level of resilience expected
- The service quality experienced by end users, and the minimum quality of service expected of undertakings' networks
- numbering issues, including the availability of numbers and number portability
- interconnection

1.1 Summary of recommendations

Our recommendations, repeated below, should be understood to be relevant to the period after transposition of the 2009 directives into Irish law.

R1. We recommend that undertakings providing PCNs or PECS should adopt best practice in relation to security and integrity, including the following matters:

- **High level security policy with very clearly defined statements of security requirements - this should include sections covering:**
  - **security governance, risk management and compliance**
  - **asset management and control**
  - **personnel security**

  - **technical information security & assurance controls**
  - **physical security**
  - **business continuity and incident management**
- **At a more detailed level, the following considerations, amongst others, may be appropriate:**
  - **requirements for patch management ensuring that all devices have the appropriate security patches applied within a suitable timeframe**
  - **the use of encryption technologies to encrypt data while in transit, and at rest while stored within applications**
  - **the structuring of networks to achieve the secure separation of data – for example separating VoIP traffic from customer data**
  - **logging and monitoring of security events to enable the detection and investigation of security incidents and breaches**
  - **incident management and reporting procedures, enabling the reporting of incidents to ComReg and the CERT as defined in the National Cyber Security Strategy**
  - **outline procedures for the independent regular auditing and vulnerability scanning of service providers security controls**

Undertakings providing PCNs or PECS should provide an annual report to ComReg documenting the approach they are taking to meeting their obligations to ensure security and integrity of their networks and services. They should also report to ComReg any significant changes to their ability to ensure security and integrity of their networks and services in a timely manner.

We note that standards for network security and integrity are under development at a European level and that it is expected that operators will monitor these developments and implement systems meeting the required standards within a reasonable period, once these European standards are finalised.

R2. **We recommend that all voice providers note their need to comply with the new regulatory framework, and meet their obligations with respect to "force majeure". Best practice to support this may include, for example, risk mitigation strategies geared towards ensuring critical points are serviced by adequate:**

  - **redundancy,**
  - **diversity,**
  - **and recovery capability**

Consideration of acceptable levels of "mean time to repair" (MTTR) may also be appropriate, as well as consideration of business continuity and disaster recovery plans.

R3. For reasons of practicality, **we recommend that ComReg allow service providers a reasonable period to introduce the measures necessary to meet their obligations.**

Improvements to policies and procedures may be achievable within a relatively short period, but the introduction of network changes to improve network security, integrity and resilience will be subject to design, procurement and implementation timescales and in some cases commercial agreement with other service providers. For these reasons we recommend that ComReg allow service providers at least 12 months to introduce all necessary measures.

R4. **ComReg should withdraw their existing access to emergency calls policy relating to ECS providers, as outlined in the VoIP guidelines (ComReg 05/50), as the obligation to provide access to emergency services now applies to all undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan.**

R5. We recommend that the competent authority should link the accuracy and reliability requirements to the ECAS specification. For example, "all fixed location PATS providers which are not nomadic providers shall provide Fixed Line Location Information to the ECAS in accordance with the ECAS RIO/LIRO, and the key local specifications referenced by the ECAS RIO". This may need to be enhanced with requirements concerning the reliability of the information.

R6. Furthermore, we recommend that a provider of PATS at a fixed location should obtain (from the customer if necessary) the physical location at which the service will normally be used before they activate a new customer's service.

R7. We recommend that providers of PATS at a fixed location should also provide one or more easy ways for their customers to update the physical location they have registered with the provider (e.g. via a secure Internet service), if it changes.

R8/9. We recommend that:

- **In the short term, where it is not technically feasible for an undertaking to provide accurate caller location information because it is VoIP originated, ComReg should allow undertakings to present these calls to the ECAS.** We note that the ECAS schedule 5 obliges the operator to provide to the ECAS provider an indicator that the call is a VoIP Originated Emergency Call.
- **In the medium term, ComReg should monitor developments in Europe and internationally and may wish to commence discussions with the DCENR in relation to the development of a national architecture, which may be similar to those developed by the NENA and NICC, for providing sufficient location information of nomadic VoIP users to the ECAS. This work could be guided by the EENA NG112 TC, and will need to accommodate the use of traditional networks and the future migration to end-to-end IP connectivity.**

R10. We recommend that until such time that a national solution for providing sufficient location information for nomadic users to the ECAS is in place, end-users of nomadic

services should be clearly informed that nomadic use of their VoIP service may not influence where a call to the emergency services is directed, i.e. the call will most likely be directed to their "home" emergency services, rather than to the emergency services appropriate to their current location.

R11. On the basis of Recital 40, **we recommend that undertakings take the "necessary measures" needed to ensure service availability and uninterrupted access to emergency services**.

R12. We recommend that service availability should be equal to that provided by broadly similar categories of voice provider:

- **voice services provided by a wired access provider should meet an availability standard equivalent to the existing PSTN. Should battery backup be required for CPE, or for remote infrastructure, the time supported by the batteries should be sufficient to cover either the great majority of repairs or provide sufficient time for end users to be warned that an alternative means of calling may need to be employed.**
- **voice services provided by wireless access providers should meet an availability standard at least equivalent to the best of existing cellular networks**
- **voice services provided by a network independent provider should seek to meet an availability level as high as is feasible given their lack of control over certain parts of the infrastructure used to provide the service. We note that these providers would be expected to make use of all appropriate techniques such as**
  - **prioritization**
  - **negotiation of suitable service level agreements.**

For the avoidance of doubt, it is not envisaged that the current level of availability will be reduced.

R13. We recommend service providers should inform their customers clearly of any ways in which the emergency calls service may not be fully equivalent to the traditional wireline PSTN. Customers should be informed in any guide issued by the service provider, and the same information should be included in materials made available to prospective customers in advance of the point of sale.

R14. To understand whether there are specific service quality issues which may make the new clause 22(3) more pertinent, we recommend that **one input which ComReg could consider before taking any further action is the volume of customer complaint data. This, amongst other considerations, may indicate whether there is a need for ComReg to set any specific quality of service requirements on undertakings providing voice services using specific technologies, such as VoIP**.

R15. As the provisions on contracts, information transparency and quality of service apply to all providers of communications networks or services, not only VoIP service providers, we recommend that in the first instance **action might be necessary to remind all providers of their duties once the 2009 Framework is transposed**.

R16. We recommend that **undertakings should be encouraged to provide terms and conditions in plain English.**

R17. As regards network neutrality we recommend that ComReg continue to monitor the market situation, but at this point we consider that no action need be taken by ComReg as the BEREC work is likely to generate a harmonised position at EU-level. Intervention should only be necessary in the case of critical failure.

R18. We believe no specific action is required for numbering regarding VoIP in relation to changes in the Directives. Aspects of existing ComReg policy relating to nomadic use (e.g. 04/103 decision 18) could be restated.

R19. As Section 4.13 of ComReg 05/50 largely reflects the requirements of Article 28, and noting that ComReg consider there to be no inconsistency in this regard, **we recommend this section should be adopted in future guidelines.**

R20. The ERG began in 2009 to consider the scope of problems associated with cross-border enforcement. During 2010/11, BEREC will continue this work and will focus particularly on the numbering aspect with reference to Article 28. **We recommend that ComReg monitor this work.**

R21. We note that the amendments to Clause 30(1) of the Universal Service Directive also mean that once transposed, **the number portability policy relating to ECS, as previously outlined in the VoIP guidelines (ComReg 05/50), is no longer applicable as number portability obligations now apply to all undertakings providing numbers from the national numbering plan.**

2 Introduction

In August 2006, ComReg published the results of its VoIP framework review in Ireland (ComReg 06/45). Since that time, in 2009, the European Commission has updated the regulatory framework.

In this context, ComReg has commissioned Analysys Mason to conduct a review of the regulation of Voice over Internet Protocol (VoIP) / Voice over Broadband (VoB) in Ireland. Our review has accounted for national developments, as informed by a series of interviews with key stakeholders in Ireland, and the activities of national regulatory authorities (NRAs) across a number of other Member States.

2.1 New regulatory framework (2009)

On 19 December 2009, the legislation comprising the new regulatory framework for telecommunications entered into force, with its publication in the Official Journal of the European Union (OJEU). This includes the following legislation:

- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (‘the Universal Service Directive, or USD’), Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (‘the e-privacy Directive’), and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws;

- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services (‘the Framework Directive’), 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

These Directives must be transposed into the national law of the EU's 27 Member States by May 2011.

This review focuses on the potential impact of the amended legislation on VoIP in Ireland. Specifically we examine:

- security and integrity of networks and services, and the new obligations faced by network operators
- access to emergency services, including the level of resilience and the provision of location information
- quality of service,
- numbering,
- and interconnection.

As legal interception (also referred to as lawful interception) is not within the remit of ComReg, it is outside of the scope of this study.

Where we make recommendations within this report based on the new directives, our recommendations should be understood to be relevant to the period after transposition of the 2009 directives into Irish law.

2.2 Report structure

The remainder of this report is therefore structured as follows:

- Section 3 assesses the new obligations on undertakings with respect to the security and integrity of networks and services
- Section 4 discusses access to emergency services and considers the ability to make emergency calls, the provision of caller location information, and the level of resilience expected by the new regulatory framework
- Section 5 assesses QoS in the context of service quality experienced by end users, and the minimum quality of service expected of undertakings' networks
- Section 6 considers numbering issues, including the availability of numbers and number portability
- Section 7 discusses interconnection
- Section 8 summarises the recommendations presented in the earlier sections.

The report also includes a number of annexes containing supplementary material:

- Annex A contains relevant text on past regulation of VoIP including excerpts from Articles and Recitals applicable under the 2002 European regulatory framework
- Annex B provides an overview of the NENA i2 architecture

3 Security and integrity of networks and services

3.1 Background

The European Commission has increasingly highlighted the importance of network and information security and resilience. Deliberate attack, disruptions due to physical phenomena, software and hardware failures, and human errors (such as incorrect configuration as well as accidental damage to underground cables) can all affect the proper functioning of public communications networks, but it is in citizens interests that the networks which form such an essential part of modern infrastructure are resilient and continue to function.

The 2002 framework sets out a variety of requirements with respect to the security and integrity of networks and services. In the context of access to emergency services, Article 23 of the USD specifically states the importance of service availability and reliability[1]. The e-privacy Directive also obliges service providers to take appropriate measures to safeguard security of services and to notify users of potential breaches of security (Recital 20, formalised by Articles 4 and 5)[1].

Other than in their VoIP guidelines (Doc 05/50[2]), which set out how service providers of VoIP services should inform their customers of the limitations of their service vis-à-vis what customers might legitimately expect compared to a PSTN-centric network, ComReg do not presently specify any further requirements in relation to network integrity.

3.2 Changes introduced by new regulatory framework

Through the changes introduced by the 2009 amendments to the regulatory framework, European telecom network operators and service providers now face new obligations regarding the security and integrity of networks and services.

Directive 2009/140/EC introduces a number of amendments in the area of security and integrity which are designed to strengthen the resilience of current electronic communications networks and systems. These amendments complement Framework Decision 2005/222/JHA[3] on attacks against information systems, which criminalises certain activities.

---

[1] See Annex A.2

[2] Subsequent Information note, published in December 2007, provided further guidance to VoIP providers in relation to their duties concerning their customers' rights regarding directory services and the prevention of unsolicited marketing calls

[3] The objective of the Council Framework Decision 2005/222/JHA of 24 February 2005 was to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

A new Chapter, *Chapter IIIa: Security and integrity of networks and services*, added to the Framework Directive introduces two new Articles relevant to this study:

- Article 13a: Security and integrity, obliging Member States to:
  - ensure that undertakings providing PCNs or PECS take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services.
  - ensure that undertakings providing PCNs take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.
  - ensure that undertakings providing PCNs or PECS notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. Where appropriate, the national regulatory authority concerned shall inform other NRAs and ENISA. The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.
  - Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

- New Article 13b: Implementation and enforcement, obliging Member States to:
  - ensure that in order to implement Article 13a, competent NRAs have the power to issue binding instructions, including those regarding time limits for implementation, to undertakings providing PCNs or PECS.
  - ensure that competent NRAs have the power to require undertakings providing PCNs or PECS to: (a) provide information needed to assess the security and/or integrity of their services and networks, including documented security policies and (b) submit to a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the national regulatory authority.
  - ensure that NRAs have all the powers necessary to investigate cases of non-compliance and the effects thereof on the security and integrity of the networks

Directive 2009/136/EC also introduces changes. Recital 35 of Directive 2009/136/EC states (emphasis added):

> In future IP networks, where provision of a service may be separated from provision of the network, **Member States should determine the most appropriate steps to be taken to ensure the availability of publicly available telephone services provided using public communications networks** and uninterrupted access to emergency services in the event of catastrophic network breakdown or in cases of force majeure, taking into account the priorities of different types of subscriber and technical limitations.

This is implemented by Article 23 of the revised USD, which states (emphasis added):

> Availability of services
>
> **Member States shall take all necessary measures to ensure the fullest possible availability of publicly available telephone services provided over public communications networks in the event of catastrophic network breakdown or in cases of force majeure.** Member States shall ensure that undertakings providing publicly available telephone services take all necessary measures to ensure uninterrupted access to emergency services.

In terms of resilient access to emergency services, these changes are also considered in Section 5 of this report.

3.3 Discussion, conclusions and recommendations

The new provisions of Articles 13a and 13b of the revised Framework Directive, together with Article 4 of the e-Privacy Directive under the 2002 regulatory framework[4], strengthen the obligations for operators to ensure security and integrity of their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities[5]. The changes reflect the package of proposals published in November 2007 in which the Commission indicated that the only way to ensure that networks are secure and services are not interrupted or lost, is to impose minimum security standards on network operators and for Member States to proactively enforce secure network design and operation.

VoIP infrastructure and services create a complex system that offers potential intruders various opportunities for attack. Whilst the PSTN is not invulnerable to security breaches, few are skilled enough or have access to the infrastructure used to manage calls. The risk of attacks against VoIP

[4] See Annex A.2

[5] ENISA is supporting the Commission and the Member States by providing its expertise in developing appropriate implementing measures.

networks may be significantly greater: VoIP systems are often connected to the Internet (and therefore can be attacked remotely and relatively anonymously); can be based on commodity hardware and in some cases commodity/open source software; and there is a lower barrier to entry (meaning service providers may employ possibly fewer, and therefore possibly more generalist, staff). Specific areas of vulnerability include:

- Configuration weaknesses in VoIP devices
- IP infrastructure attacks, such as any Distributed DoS (DDoS), SYN floods or other traffic surge attacks that exhaust network resources and could severely impact VoIP communications
- VoIP application level attacks, such as call hijacking, eavesdropping, and message integrity attacks

Article 23 of the revised USD obliges Member States to take "all necessary measures" to ensure availability of services and uninterrupted access to emergency services. In determining how to secure VoIP, service providers need to proactively identify and fix VoIP-specific vulnerabilities before they impact end users. Vulnerability assessment, a commonly used approach from the data security world, could be a particularly effective proactive strategy. Once vulnerabilities are identified they should be addressed by appropriate actions, although any security architectures and solutions deployed must not impact VoIP service quality and reliability.

As the popularity of VoIP increases, so will its exposure to current and emerging security threats. Security countermeasures for VoIP will therefore require a careful balance between policies, procedures, and technology solutions. However, the obligations of Articles 13a and 13b extend to all operators and with the migration to IP-centric networks, and with an increased focus on security and integrity, these issues will become relevant to the entire industry.

R1. We therefore recommend that undertakings providing PCNs or PECS should adopt best practice in relation to security and integrity, including the following matters:

- **High level security policy with very clearly defined statements of security requirements - this should include sections covering:**
  - **security governance, risk management and compliance**
  - **asset management and control**
  - **personnel security**
  - **technical information security & assurance controls**
  - **physical security**
  - **business continuity and incident management**
- **At a more detailed level, the following considerations, amongst others, may be appropriate:**
  - **requirements for patch management ensuring that all devices have the appropriate security patches applied within a suitable timeframe**

- **the use of encryption technologies to encrypt data while in transit, and at rest while stored within applications**
- **the structuring of networks to achieve the secure separation of data – for example separating VoIP traffic from customer data**
- **logging and monitoring of security events to enable the detection and investigation of security incidents and breaches**
- **incident management and reporting procedures, enabling the reporting of incidents to ComReg and the CERT as defined in the National Cyber Security Strategy[6]**
- **outline procedures for the independent regular auditing and vulnerability scanning of service providers security controls**

Undertakings providing PCNs or PECS should provide an annual report to ComReg documenting the approach they are taking to meeting their obligations to ensure security and integrity of their networks and services. They should also report to ComReg any significant changes to their ability to ensure security and integrity of their networks and services in a timely manner.

We note that standards for network security and integrity are under development at a European level and that it is expected that operators will monitor these developments and implement systems meeting the required standards within a reasonable period, once these European standards are finalised.

The "force majeure" provision in Article 23 of the USD is relevant insofar as the associated obligations may be new to those ECS providers which will become PATS as a result of the amendment in the PATS definition.

R2. **We therefore recommend that all voice providers note their need to comply with the new regulatory framework, and meet their obligations with respect to "force majeure". Best practice to support this may include, for example, risk mitigation strategies geared towards ensuring critical points are serviced by adequate:**

- **redundancy,**
- **diversity,**
- **and recovery capability**

Consideration of acceptable levels of "mean time to repair" (MTTR) may also be appropriate, as well as consideration of business continuity and disaster recovery plans.

The following standards may have useful role:

- BS25777

[6] DCENR National Cyber Security Strategy

- BS25999
- ISO 27001

R3. For reasons of practicality, **we also recommend that ComReg allow service providers a reasonable period to introduce the measures necessary to meet their obligations. Improvements to policies and procedures may be achievable within a relatively short period, but the introduction of network changes to improve network security, integrity and resilience will be subject to design, procurement and implementation timescales and in some cases commercial agreement with other service providers. For these reasons we recommend that ComReg allow service providers at least 12 months to introduce all necessary measures.**

4 Access to emergency services

4.1 Introduction

The new regulatory framework aims to ensure that citizens gain better access to emergency services by extending the access requirements from traditional telephony to new technologies, strengthening operators' obligations to pass information about caller location to emergency authorities, and by improving general availability and reliability of access. We therefore discuss access to emergency services in several parts:

- The ability to make a call to the emergency services
- The provision of location information
- The availability and reliability of access

4.2 The ability to make a call to emergency services

4.2.1 Background

In Article 2 of the Universal Service Directive (2002/22/EC), *publicly available telephone service (PATS)* was defined as follows (emphasis added):

> "publicly available telephone service" means a service available to the public for originating and receiving national and international calls **and access to emergency services through a number or numbers in a national or international telephone numbering plan**…"

USD Article 26 (Single European emergency call number) requires that (emphasis added):

> "1. Member States shall ensure that, in addition to any other national emergency call numbers specified by the national regulatory authorities, **all end-users of publicly available telephone services**, including users of public pay telephones, **are able to call the emergency services** free of charge, by using the single European emergency call number "112"."

Provision of access to emergency services was therefore linked to the definition of PATS, which carried additional rights and obligations.

As a result, there were concerns regarding:

- **Consumer education**. Users receiving a service that did use telephone numbers but did not provide access to emergency services might be unaware of this and find themselves unable to make a call to the emergency services at the critical moment
- **Incentives**. The additional rights and obligations of PATS providers might provide a disincentive to providing access to emergency service.

ComReg presently require service providers who offer a service classified as PATS to offer guaranteed, free-of-charge access to emergency service numbers 112 and 999. Service providers who offer services classified as ECS, and that use numbers, are advised that they must ensure customers are advised of any limitations of their services, including, but not limited to, the provision of access to the emergency services[7].

ComReg 05/50 (which is non-binding) also discusses the possibility of an ECS VoIP (i.e. non-PATS) provider offering what it calls "best efforts access to emergency calls (for ECS only)". Providers are encouraged to offer access, and to inform the customer of the characteristics of the service offered via the user guide and via the distribution of stickers. In this way the incentives issue and the consumer protection issue were both addressed.

4.2.2 Changes introduced by new regulatory framework

The Universal Service Directive, as amended by Directive 2009/136/EC, defines PATS as:

> ""publicly available telephone service" means a service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan"

The ability to provide access to the emergency services has therefore been removed as a factor in the definition of PATS.

Article 26(2) of the amended Universal Service Directive further ensures that users of a service offering outgoing calls (note: PATS is not stated) are able to access emergency services (emphasis added):

> "2. Member States, in consultation with national regulatory authorities, emergency services and providers, shall ensure that undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan **provide access to emergency services**."

Article 26(4) also introduces a new requirement in relation to access for disabled end users. This has no impact that is specific to VoIP providers.

[7] ComReg 05/50

4.2.3 Discussion, conclusions and recommendations

The amendment in the definition of PATS has significant implications for those operators currently deemed a provider of publicly available ECS. In practice, we expect that all VoIP service providers in Ireland who allow calls to telephone numbers will now be categorised as PATS providers, and in turn be subject to the rights and obligations under the new regulatory framework including the obligation to ensure uninterrupted access to emergency services.

R4. Therefore, **ComReg should withdraw their existing access to emergency calls policy relating to ECS providers, as outlined in the VoIP guidelines (ComReg 05/50), as the obligation to provide access to emergency services now applies to all undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan.**

4.3 Provision of location information

4.3.1 Background

Article 26 of the Universal Service Directive (2002/22/EC) (Single European emergency call number) requires that (emphasis added):

> "3. Member States shall ensure that **undertakings which operate public telephone networks make caller location information available to authorities handling emergencies, to the extent technically feasible,** for all calls to the single European emergency call number "112"."

There is a policy reason in favour of ensuring that location information is available to the emergency services when an end user calls 112 or 999, as a small percentage of callers are not able to give an accurate indication of their location. These may include calls from very young children, medical emergencies where the caller is incapacitated, or cases in which the caller needs to remain hidden and silent.

For the fixed network, the caller's location information can usually be provided to the emergency services. However, calls from corporate telephony networks, mobile networks, and nomadic or potentially nomadic users, pose additional difficulties.

ComReg presently requires those undertakings operating PTNs (i.e. an electronic communications network which is used to provide PATS) must, as soon as practicable, make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls to 112 and 999.

The new ECAS[8], due to replace the 999 service currently provided by eircom, will maintain a number of databases for the purposes of determining caller location including the ECAS Fixed Line Information Database, and the ECAS Mobile Location Information Conversion Database.

ECAS

To provide legal and regulatory certainty BT will be entering into contracts with the providers supplying 112/999 calls or location information to ECAS and these contracts will be known as the Reference Interconnect Offer (RIO) for providers directly interconnecting to the BT ECAS, and the Location Information Reference Offer (LIRO) for providers not directly interconnected, but using the BT ECAS to fulfil their access to emergency services obligations. The RIO incorporates the LIRO.

The Fixed Location Information Specification document sets out the format and definition of location information records to be contained in the ECAS Fixed Line Information Database, and the approach and requirements for the transfer of this information to ECAS is detailed in the "ECAS Data Transfer Specifications" document.

For VoIP, the ECAS Schedule 5[9] specifies that:

> In the event that BT receives a VoIP Originated Emergency Call for which it is not possible to clearly confirm the location and appropriate Connect To Number[10], or the information is incorrect or corrupted, BT shall use reasonable endeavours to convey the Call to a Connect To Number for the appropriate Emergency Service.

[8] Following the introduction of the Communications Regulation (Amendment) Act of 2007, the Department of Communications, Energy and Natural Resources (DCENR) tendered for a supplier to provide the Emergency Call Answering Service (ECAS) for Ireland. On completion of this open tender process BT was awarded the contract (known as a Concession Agreement) to provide 112 and 999 call answering services on behalf of the State of Ireland.

[9] http://www.btwholesale.ie/images/ECASRIOSchedule5ExecutionVersionGenericv32.pdf

[10] 'Connect To Number' is the number, based upon the location information available, in the ECAS Emergency Routing Database for the emergency service requested by the caller

It also obliges the operator to provide to the ECAS provider:

> - a telephone number that may be used to call the Customer;
>
> - an indicator that the call is a VoIP Originated Emergency Call;
>
> - the Customer's name and billing address. Where available to the Operator (either through the customer informing the Operator or the address being known by the Operator) the installation address should be provided. For Customers with nomadic applications that use more than one Network Termination Point, the installation address is (until dynamic methods to update the address can be agreed) the address where the application is normally used.

We understand from our stakeholder interviews that the ECAS provider will question the caller as to their location for any call marked as VoIP originated. If unsuccessful in gaining this information they will connect a nomadic user to the Connect To Number for the emergency service covering their installation address.

Technological developments in relation to caller location information

In most European countries the location information of VoIP calls directed to 112/999 is found by the emergency response centre by looking up the telephone number in a database[11] or requiring such information from the operator that provides the service to the customer.

It is, however, technically difficult to reliably determine the location of the caller if the VoIP service is used nomadically as the caller's IP address is assigned dynamically and not tied to a specific location.

VoIP services depend on a multi-layered network architecture. The caller's location is only directly related to their current physical network access and therefore only reliably known by the access network provider. Furthermore a VoIP customer may move from one physical access point to another (or even from one ISP to another) without the VoIP provider's knowledge. Therefore the VoIP service provider (VSP), ISP and access network provider must all cooperate to determine the caller's current location and supply it to the emergency handling authorities.

Annex B provides an overview of the current situation in relation to standardisation and a high level discussion of the i2 architecture, highlighting the main functional elements used to support validation and management of location information.

[11] The ECAS will maintain a number of databases for the purposes of determining caller location including the ECAS Fixed Line Information Database, and the ECAS Mobile Location Information Conversion Database.

4.3.2 Changes introduced by new regulatory framework

Article 26(5) of the amended Universal Service Directive (Emergency services and the single European emergency call number) updates the previous requirement relating to the provision of caller location information (emphasis added):

> "5. Member States shall ensure that **undertakings concerned make caller location information available free of charge** to the authority handling emergency calls as soon as the call reaches that authority. This shall apply to all calls to the single European emergency call number '112'. Member States may extend this obligation to cover calls to national emergency numbers. **Competent regulatory authorities shall lay down criteria for the accuracy and reliability of the caller location information provided.**"

The amendment makes it very clear that undertakings "concerned" must make caller location information available to the authority handling emergency calls. Whilst at the moment a single undertaking might be "concerned" in a single case (as explained in Section 4.3.1), this might in future include multiple operators in a single case (e.g. if a nomadic user is using a WiFi hotspot provided by a third party).

As 999 and 112 exist equally and run in parallel in Ireland, it is highly likely that the obligation introduced by Article 26(5) will be extended to 999 calls.

Recital 39 of Directive 2009/136/EC provides additional clarity on the provision of caller location information (emphasis added):

> ….The obligation to provide caller location information should be strengthened so as to increase the protection of citizens. In particular, **undertakings should make caller location information available to emergency services as soon as the call reaches that service independently of the technology used**. **In order to respond to technological developments, including those leading to increasingly accurate caller location information, the Commission should be empowered to adopt technical implementing measures to ensure effective access to '112' services** in the Community for the benefit of citizens. Such measures should be without prejudice to the organisation of emergency services of Member States.

However, Recital 40 of Directive 2009/136/EC clearly acknowledges limitations for network independent undertakings in this regard (emphasis added).

> (40) Member States should ensure that undertakings providing end-users with an electronic communications service designed for originating calls through a number or numbers in a national telephone numbering plan provide reliable and accurate access to emergency services, taking into account national specifications and criteria. Network-independent undertakings may not have control over networks and may not be able to ensure that emergency calls made through their service are routed with the same reliability, as they may not be able to guarantee service availability, given that problems related to infrastructure are not under their control. **For network-independent undertakings, caller location information may not always be technically feasible. Once internationally-recognised standards ensuring accurate and reliable routing and connection to the emergency services are in place, network-independent undertakings should also fulfil the obligations** related to caller location information at a level comparable to that required of other undertakings.

4.3.3 Discussion, conclusions and recommendations

The key difference between the 2002 and 2009 Frameworks is that previously the text was "make caller location information available … to the extent technically feasible", whereas the text now says "Competent regulatory authorities shall lay down criteria for the accuracy and reliability of the caller location information provided".

Post-transposition it is possible that ComReg will be considered the competent regulatory authority under article 26(5), and thereby gain a duty to "lay down criteria for the accuracy and reliability of the caller location information provided".

In the short term this divides into a number of specific issues for ComReg to consider:

- The accuracy and reliability of the information passed by fixed operators (in essence, the accuracy of the address database used). This is not an issue only for VoIP service providers, but it may require ComReg to monitor the levels of accuracy and reliability.
- The accuracy of the information provided by MNOs. We understand that presently information is provided based on Cell ID. However, over time equipment vendors and MNOs will develop systems capable of providing caller location information with increasing accuracy, and ComReg may wish to consider mandating these in the future; matching changes to the ECAS service would also be needed in this case, but we understand this is already provided for in the ECAS Schedule 5.

- Whether it is acceptable to have no location information (or potentially inaccurate location information) provided in the case of nomadic VoIP users, and how these can be distinguished from non-nomadic VoIP user for which a similar level of accuracy to other fixed networks should be possible.

R5. We recommend that the competent authority should link the accuracy and reliability requirements to the ECAS specification. For example, "all fixed location PATS providers which are not nomadic providers shall provide Fixed Line Location Information to the ECAS in accordance with the ECAS RIO/LIRO, and the key local specifications referenced by the ECAS RIO". This may need to be enhanced with requirements concerning the reliability of the information.

R6. Furthermore, we recommend that a provider of PATS at a fixed location should obtain (from the customer if necessary) the physical location at which the service will normally be used before they activate a new customer's service. This is a more demanding requirement than in ComReg 05/50. However, as it is in line with the requirements of the ECAS contracts, it may not be necessary for ComReg to demand it as it may be enforced through the ECAS contracts.

R7. We also recommend that providers of PATS at a fixed location should also provide one or more easy ways for their customers to update the physical location they have registered with the provider (e.g. via a secure Internet service), if it changes.

It is worth noting that our interviews with stakeholders demonstrated an encouragingly high participation by VoIP providers in the testing of the ECAS system, with many service providers already providing caller location information in accordance with the ECAS specifications.

The work done in the US (NENA i2/i3), Canada ("Canadian i2" architecture), and the UK (NICC), has shown that national models for joining together the links in the information chain in order that emergency services may have location information provided are beginning to mature. A number of vendors have also designed products to meet these architectures, including Andrew[12] and RedSky Technologies[13]. However, it will take some time to phase in a national solution – as well as the time needed to develop and agree a suitable architecture, service providers will need time to accommodate the resulting changes to their networks and operational models, and time will also be need to verify the interoperability of solutions. In addition, consideration needs to be given to the continued use of traditional networks to convey calls to the emergency services. Whilst this reflects the status quo and probably the situation for the immediately foreseeable future, it is important to recognise that in due course there will be a desire to move to end-to-end IP connectivity for emergency calls.

[12] http://www.commscope.com/company/eng/index.html

[13] http://www.redskye911.com/

R8/9. We therefore recommend that:

- **In the short term, where it is not technically feasible for an undertaking to provide accurate caller location information because it is VoIP originated, ComReg should allow undertakings to present these calls to the ECAS.** We note that the ECAS schedule 5 obliges the operator to provide to the ECAS provider an indicator that the call is a VoIP Originated Emergency Call.
- **In the medium term, ComReg should monitor developments in Europe and internationally and may wish to commence discussions with the DCENR in relation to the development of a national architecture, which may be similar to those developed by the NENA and NICC, for providing sufficient location information of nomadic VoIP users to the ECAS. This work could be guided by the EENA NG112 TC, and will need to accommodate the use of traditional networks and the future migration to end-to-end IP connectivity.**

Under ComReg 05/50, service providers are presently obliged to inform customers what would happen if nomadic use is envisaged:

> End-users of both PATS and ECS services should also be clearly informed that nomadic[6] use of their VoIP service may not influence where a call to the emergency services is directed, i.e. the call will most likely be directed to their "home" emergency services, rather than to the emergency services appropriate to their current location.

R10. We recommend that until such time that a national solution for providing sufficient location information for nomadic users to the ECAS is in place, end-users of nomadic services should be clearly informed that nomadic use of their VoIP service may not influence where a call to the emergency services is directed, i.e. the call will most likely be directed to their "home" emergency services, rather than to the emergency services appropriate to their current location.

4.4 Availability and reliability of access

4.4.1 Background

Article 23 of the Universal Service Directive (2002/22/EC) (Integrity of the network) requires that (emphasis added):

> "Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or **in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations.** Member States shall ensure that undertakings providing publicly available telephone services at fixed locations take **all reasonable steps** to ensure uninterrupted access to emergency services."

ComReg presently requires that undertakings providing PATS at fixed locations shall take all reasonable steps to ensure uninterrupted access to emergency services.

In 05/50 (Section 4.5), ComReg gives some non-binding guidance relating to access to emergency services from ECS, including what it describes as "best efforts access to emergency services".

ECAS

To ensure uninterrupted access to the emergency services, the ECAS design and structure is engineered to provide 99.999% availability[14], with 3 PSAPs (located in Ballyshannon, Navan, and Dublin Eastpoint) and 2 geographically separate equipment centres (Navan and Dublin Citywest).

The operation of the service conforms to the following standards[13]:

- Information security management ISO 17799 and ISO 27001
- Business continuity BS 25999-1 and BS 25999-2
- ISO 9001:2000

4.4.2 Changes introduced by new regulatory framework

Article 23 of the amended Universal Service Directive (Availability of services) updates the previous requirement (emphasis added):

[14] Source: DCENR, ComReg

> "Member States shall take all necessary measures to ensure the **fullest possible availability** of publicly available telephone services provided over public communications networks in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that undertakings providing publicly available telephone services take **all necessary measures** to ensure uninterrupted access to emergency services."

Recital 40 of Directive 2009/136/EC clearly acknowledges limitations for network independent undertakings on reliability (emphasis added).

> ... **Network-independent undertakings** may not have control over networks and may not be able to ensure that emergency calls made through their service are routed with the same reliability, as they **may not be able to guarantee service availability,** given that problems related to infrastructure are not under their control. …

4.4.3 Discussion, conclusions, and recommendations

VoIP as a technology allows new system architectures, including those in which the voice service provider has no direct association with the access network (which for example allows nomadic use), where call data packets may travel over best-effort Internet interconnections and be mixed with "bursty" traffic, and the service provider may be unable to prioritise the traffic until it reaches its own infrastructure. There is therefore a concern that the current high standard access (resilient, prioritised, and often with access to location information) to the emergency services might be degraded by a shift to VoIP. This risk is, however, sometimes overstated because:

- Mobile telephony exists.
  - Given the high mobile penetration and extensive network coverage in Ireland, most fixed line users have a mobile phone alternative, even if indoor coverage is less than optimal in some locations. This makes the system as a whole more resilient as users generally have two or more relatively independent means of making calls to the emergency services[15]
  - Many calls to the emergency services today use mobile handsets and networks, which can experience reliability problems (e.g. battery too low; no signal in some locations; base station failure). This has not been considered a reason to require increased resilience from mobile networks, although the removal of "at a fixed location" from Article 23 now means that mobile PATS is now within scope and as a result MNOs may be under greater obligations.

[15] Calls to 112 [DRAFTING NOTE and 999] in Ireland may work if the mobile phone is within the range of any network, even if the one the user is subscribed to is out of range. Mobile phones without a SIM card can also make emergency calls as long as the battery has power.

- Some fixed location users use handsets (e.g. DECT handsets) which are battery powered and where the wireless base unit requires mains power. These systems do not work in the case of local power failure or low battery - nevertheless they are popular with users.
- Despite its high standard, even the fixed network is not fully resilient. For example, 1-in-1000 year floods may flood a remote site; it could be fire damaged; or a small remote exchange may not have a resilient link to the core network, so its link could be broken for example through accidental contact with underground cabling during excavation work.

The question is: what measures are necessary to ensure uninterrupted access, and how can this be expressed in a way that broadly maintains the current high level of availability whilst taking into account the capabilities of multiple technologies (PSTN, mobile, VoIP) whilst allowing technology change?

With the changes introduced by the new regulatory framework, Member States no longer have to "ensure... the availability" of the public telephone network and publicly available telephone services at fixed locations in the event of catastrophic network breakdown or in cases of force majeure. Instead they are obliged to "take all necessary measures" to ensure the **fullest possible** availability of publicly available telephone services provided over public communications networks in the event of catastrophic network breakdown or in cases of force majeure. (emphasis added)".

This change raises two interesting points:

- "fullest possible" suggests that "full" may not be possible.
- for the undertakings providing publicly available telephone services, "all reasonable steps" has been replaced with "all necessary measures" (although we note Recital 35 of Directive 2009/136/EC says still says "reasonable steps").

R11. On the basis of Recital 40, **we recommend that undertakings take the "necessary measures" needed to ensure service availability and uninterrupted access to emergency services**.

The extent of the measures necessary must be determined by the undertaking, and will depend on network architecture and device capabilities. For example, we note that a service for a network independent smartphone application (such as the Truphone mobile VoIP[16] client) may be able to meet this requirement by the application closing and the emergency call being routed via the cellular network to which the device is connected.

[16] Mobile VoIP is a term used to describe the delivery of VoIP over a mobile network. Mobile VoIP is generally delivered by a third party service provider over a Wi-Fi or cellular network to which the mobile device is connected

The measures required may also change over time, especially in the case of network independent providers as it may become feasible in future to improve the availability over the current level (e.g. by prioritising voice data packets, or prioritising emergency calls in particular).

R12. We recommend that service availability should be equal to that provided by broadly similar categories of voice provider:

- **voice services provided by a wired access provider should meet an availability standard equivalent to the existing PSTN. Should battery backup be required for CPE, or for remote infrastructure, the time supported by the batteries should be sufficient to cover either the great majority of repairs or provide sufficient time for end users to be warned that an alternative means of calling may need to be employed.**
- **voice services provided by wireless access providers should meet an availability standard at least equivalent to the best of existing cellular networks**
- **voice services provided by a network independent provider should seek to meet an availability level as high as is feasible given their lack of control over certain parts of the infrastructure used to provide the service. We note that these providers would be expected to make use of all appropriate techniques such as**
  - **prioritization**
  - **negotiation of suitable service level agreements.**

For the avoidance of doubt, it is not envisaged that the current level of availability will be reduced.

It should be noted that our interviews with stakeholders demonstrated an encouragingly high standard of network availability and integrity being sought, as these were considered essential for competitive reasons.

With respect to differences in reliability, ComReg 05/50, Section 4.5.2, indicates (emphasis added):

---

1. Where the service does provide access to '112' and '999' but **does not offer substantially the same level of reliability as circuit switched public telephony, clear information to this effect must be provided to all potential users of the service** in any user guide issued by the SP. The **same information should also be included in materials describing the service that are made available to prospective customers in advance of the point of sale.**

2. It is a strongly recommended practice, that where the service is expected to be significantly used in place of a Home Telephone in a residential environment, the SP will offer the customer a supply of **stickers which clearly indicate that calls to emergency**

services may fail, in particular if there is a loss of power or a fault in the packet data network….

Given that VoIP service providers will be under the same obligations regarding resilience of access to emergency services as other providers of PATS, it is questionable whether their customers still need to be informed of any specific issues regarding their service. However, Recital 40 does acknowledge that network-independent undertakings may not be able to guarantee service availability, given that problems related to infrastructure are not under their control – an example of this is where a network-independent VoIP service provider relies on the public Internet to transit voice traffic.

R13. On balance, **we therefore recommend service providers should inform their customers clearly of any ways in which the emergency calls service may not be fully equivalent to the traditional wireline PSTN**. **Customers should be informed in any guide issued by the service provider, and the same information should be included in materials made available to prospective customers in advance of the point of sale.**

5 Quality of Service

5.1 Introduction

The 2009 reforms strengthen the powers of NRAs to intervene where they consider that the manner in which operators handle the flow of traffic over their networks may degrade the quality of service available to subscribers. Quality of Service has two distinct meanings in this context:

- The service quality experienced by end users
- The minimum quality of service provided within the network, and its impact on users' choice of applications and services, especially those provided by third parties

5.2 Service quality experienced by end users

5.2.1 Background

The Universal Service Directive (2002/22/EC) obliged NRAs to require providers of publicly available electronic communications services to publish comparable, adequate and up-to-date information for end users on the quality of their services[17], the aim being to ensure that end users had access to comprehensive, comparable and user friendly information.

ComReg presently advises, through the 05/50 guidelines, VoIP service providers to prepare potential new customers for any limitations on quality that they might experience in using the services provided, where these might otherwise be likely to lead to complaints or dissatisfaction. In particular, impacts of latency or problems associated with packet loss should be considered. The customer must be advised of these issues at the point of sale.

[17] Articles 11 and 22

5.2.2 Changes introduced by new regulatory framework

Directive 2009/136/EC introduces, amongst other measures, the following amendments:

Changes to Article 20 (Contracts) (emphasis added):

---

1. Member States shall ensure that, when subscribing to services providing connection to a public communications network and/or publicly available electronic communications services, consumers, and other end-users so requesting, have a right to a contract with an undertaking or undertakings providing such connection and/or services. The **contract shall specify** in a clear, comprehensive and easily accessible form at least:

…

(b) the services provided, including in particular,

— **whether or not access to emergency services and caller location information is being provided, and any limitations on the provision of emergency services** under Article 26,

— **information on any other conditions limiting access to and/or use of services and applications**, where such conditions are permitted under national law in accordance with Community law,

— **the minimum service quality levels offered**, namely the time for the initial connection and, where appropriate, **other quality of service parameters, as defined by the national regulatory authorities**,

— **information on any procedures** put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures **could impact on service quality**,

…

(h) **the type of action that might be taken by the undertaking in reaction to security or integrity incidents or threats and vulnerabilities**.

Changes to Article 21 (Transparency and publication of information) gives NRAs the powers to oblige undertakings to inform subscribers of any changes to the information specified in contracts relating to, inter alia, access to emergency services, caller location information, conditions limiting access to and/or use of services, and procedures to measure and shape traffic.

Changes to the first two clauses of Article 22 (Quality of service) introduce new requirements in relation to the publication of QoS information for disabled end users. These have no impact that is specific to VoIP providers.

Directive 2009/136/EC also introduces a new clause 22(3) (emphasis added):

> 3. **In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements** on an undertaking or undertakings providing public communications networks.
>
> National regulatory authorities shall provide the Commission, in good time before setting any such requirements, with a summary of the grounds for action, the envisaged requirements and the proposed course of action. This information shall also be made available to the Body of European Regulators for Electronic Communications (BEREC). The Commission may, having examined such information, make comments or recommendations thereupon, in particular to ensure that the envisaged requirements do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements.

5.2.3 Discussion, conclusions, and recommendations

These changes, whilst significant, are not just relevant to VoIP, as they apply to all publicly available ECS. However, there is an issue relating specifically to VoIP: the contracts and transparency clauses specifically discuss "whether or not access to emergency services and caller location information is being provided, and any limitations on the provision of emergency services". This is additional evidence, in addition to Recital 40 of Directive 2009//136/EC, to support the flexible application of the Framework allowing for different levels of resilience in access to emergency services provided using, for example, fixed PSTN, PSTN/wireless handset, mobile and VoIP, and that consumers should be informed of these differences.

R14. To understand whether there are specific service quality issues which may make the new clause 22(3) more pertinent, **one input which ComReg could consider before taking any further action is the volume of customer complaint data. This, amongst other considerations, may indicate whether there is a need for ComReg to set any specific quality of service requirements on undertakings providing voice services using specific technologies, such as VoIP**.

R15. As the provisions on contracts, information transparency and quality of service apply to all providers of communications networks or services, not only VoIP service providers, in the first instance action might be necessary **to remind all providers of their duties once the 2009 Framework is transposed**.

The transparency requirements introduced by Directive 2009/136/EC oblige undertakings to:

- provide applicable tariff information to subscribers regarding any number or service subject to particular pricing conditions; with respect to individual categories of services, national regulatory authorities may require such information to be provided immediately prior to connecting the call;
- inform subscribers of any change to access to emergency services or caller location information in the service to which they have subscribed;
- inform subscribers of any change to conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law;
- provide information on any procedures put in place by the provider to measure and shape traffic so as to avoid filling or overfilling a network link, and on how those procedures could impact on service quality;
- inform subscribers of their right to determine whether or not to include their personal data in a directory, and of the types of data concerned, in accordance with Article 12 of Directive 2002/58/EC (Directive on privacy and electronic communications); and
- regularly inform disabled subscribers of details of products and services designed for them.

As per ComReg document 07/49, the terms and conditions of any contract should contain, at a minimum:

a) The identity and address of the supplier,
b) Services provided, the service quality levels offered, as well as the time for the initial connection,
c) The types of maintenance service offered,
d) Particulars of prices and tariffs and the means by which up to date information on all applicable tariffs and maintenance charges may be obtained,
e) The duration of the contract, conditions for renewal and termination of services of the contract,
f) Any compensation and refund arrangements which apply if contracted service quality levels are not met, and
g) The method of initiating procedures for settlement of disputes in accordance with Regulation 28.

R16. In addition, we recommend that **undertakings should also be encouraged to provide terms and conditions in plain English.**

5.3 Minimum quality of service provided and its impact on end-user choice

5.3.1 Background

The so-called "Net Neutrality" debate focuses on the extent to which Internet access service providers can legitimately block or degrade certain types of traffic. In particular, concerns have been raised where voice or video providers who also provide Internet access services block Internet services and applications which compete with their own retail services.

Whilst the 2002 Framework does not directly address this issue in the Articles, Recital 6 of the 2002 Access Directive (2002/19/EC) indicates (emphasis added):

> In markets where there continue to be large differences in negotiating power between undertakings, and where some undertakings rely on infrastructure provided by others for delivery of their services, it is appropriate to establish a framework to ensure that the market functions effectively. National regulatory authorities should have the power to secure, where commercial negotiation fails, adequate access and interconnection and interoperability of services in the interest of end-users. In particular, they may ensure end-to-end connectivity by imposing proportionate obligations on undertakings that control access to end-users. Control of means of access may entail ownership or control of the physical link to the end-user (either fixed or mobile), and/or the ability to change or withdraw the national number or numbers needed to access an end-user's network termination point. **This would be the case for example if network operators were to restrict unreasonably end-user choice for access to Internet portals and services.**

Accordingly there is some ability within the 2002 framework to protect end-user access to applications and services.

5.3.2 Changes introduced by new regulatory framework

In its impact assessment in 2007[18] the Commission considered that the existing rules in EC law can sufficiently deal with network neutrality problems with the exception of problems in relation to degradation of the quality of service to unacceptably low levels.

The 2002 regulatory framework does not provide NRAs with the means to intervene if the quality of service for transmission were to be degraded to unacceptably low levels, thereby frustrating the delivery of services from third parties. The impact of prioritisation or of systematic degradation of

[18] Commission Staff Working Document, Impact Assessment - Accompanying document to the Commission proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/19/EC, 2002/20/EC and 202/21/EC, SEC(2007)1472

connectivity is obviously larger on services needing real-time communications such as VoIP, in which latency is critical, and could ultimately affect end-user choice.

In summary, the Commission has introduced four specific measures with the aim of safeguarding basic access and quality of service:

- A new Framework Directive Article 8(4(g)) requires national authorities to promote "the ability of end users to access and distribute information or run applications and services of their choice."

- A revised USD Directive Article 20 obliging Member States to ensure that when entering into contracts subscribing to services providing connection to a public communications network and/or publicly available electronic communications services, consumers, and other end users are clearly informed of any conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law

- A revised USD Directive Article 21 provides similar transparency obligations to inform customers over (amongst other things)

  – restrictions on use of applications,
  – and traffic management policies

- A new USD Directive Article 22(3) granting to NRAs the power to prevent degradation of quality of service and slowing of traffic over networks by setting minimum quality levels and at the same time provide the possibility for the Commission to take implementing measures in this area

The new regulatory objective (Framework Directive Article 8(4)) to promote "the ability of end users to access and distribute information or run applications and services of their choice." and the quality of service provisions in Article 22 permits the NRA to set minimum quality of service requirements for an undertaking or undertakings providing public communications networks in order to prevent the degradation of service and the hindering or slowing down of traffic over networks. In combination these allow the NRA to take a new form of ex-ante action (which does not require a finding of SMP) to support access to network-independent applications and services

The Commission hopes that these tools can be used to combat threats to network neutrality.

5.3.3 Discussion, conclusions and recommendations

These changes, whilst significant, are not just relevant to VoIP, as they apply to all publicly available ECS. However, there is an issue relating specifically to VoIP because VoIP can be provided in a network independent way (i.e. over the top of existing networks, fixed or mobile).

There is however a wide list of such potential applications which extends way beyond VoIP: for example, IM and over-the-top video such as Hulu or Joost.

Due to the relatively low retail price of mobile data (a low average price per bit, and a very low marginal price per bit on bundled packages (i.e. zero marginal price in the bundle)), and the relatively high retail price of mobile voice, there is an arbitrage opportunity related to the use of VoIP on mobile phones. Whilst at the retail level 3 Ireland has embraced VoIP (see 3 Mobile's Skype Proposition[19]), other MNOs in Ireland impose restrictions on the use of VoIP. For example, Meteor has explicitly forbidden the use of VoIP in their terms of use of their Unlimited Mobile Internet Add-On[20], whilst O2 Ireland's iPhone Prepay service, which allows customers to use Bitbuzz's networks, forbids the enabling of VoIP under their 'Fair Usage Policy'[21] – although we have noted that O2 Ireland has very recently partnered with iSkoot to launch *O2 Social Link* which is reportedly going to support VoIP services. Vodafone Ireland has offered the ability to use VoIP but as a higher price option[22].

In the past, outside Ireland, some MNOs have disabled SIP functionality in handsets they have subsidised (for example, in 2007 it was reported that Vodafone and Orange in the UK removed the SIP functionality from the Nokia N95). There have been other instances of MNOs obstructing VoIP, such as the disputes Truphone has had with T-Mobile and Vodafone in the UK over the blocking of numbers.

What the European Commission has not defined, however, is the process by which the NRA can decide whether the setting of minimum quality of service requirements is necessary and proportionate, and how it can take account of the specific characteristics of the networks themselves and the market in which these services are offered - although early notification with the Commission and taking the utmost account of Commission comments is required (i.e. a consultation process similar to the Article 7 procedure[23]).

[19] http://www.three.ie/skype.htm

[20] http://www.meteor.ie/plans/bill_pay/add_ons/data_add_ons/dataaddons_tandcs/

[21] http://www.o2online.ie/wps/wcm/connect/O2/About+O2/Terms+and+Conditions/Promotions/

[22] http://www.vodafone.ie/terms/paymonthly/index.jsp 6652" Calling over the internet (VoIP - Voice over Internet Protocol) and data sharing (Peer to Peer) is not supported by the Vodafone's Unlimited Mobile Broadband Tariff. If you want to use such services you should purchase the tailored add-on in this regard".

[23] Article 7 of the Framework Directive gives the European Commission the powers to oversee draft national regulatory measures through a consultation at EU level. This review mechanism is intended to consolidate and safeguard the internal market. The role of the Commission is decisive, to ensure consistent regulation and to bring more transparency into the regulatory process.

We note the BEREC plans to look into the implementation of the rules of the revised regulatory framework as concerns minimum quality of service and access to Internet applications and content, and it is appropriate for ComReg to take account of this on-going work and any other guidance which may be provided by the European Commission, including *inter alia* the process by which the need to act in this area might be determined.

R17. We therefore recommend that ComReg continue to monitor the market situation, but at this point we consider that no action need be taken by ComReg as the BEREC work is likely to generate a harmonised position at EU-level. Intervention should only be necessary in the case of critical failure.

6 Numbering and related issues

6.1 Introduction

Various amendments have been made to the Directives in relation to numbering, such as the introduction of harmonised numbers for harmonised services of social value, including the missing children hotline number, and access to the European Telephony Numbering Space (ETNS). However, in this section we consider only the numbering related changes which are relevant in the context of the review of the regulatory framework for VoIP in Ireland.

6.2 Availability of numbers to service providers

6.2.1 Background

In 2004, ComReg decided to designate a new non-geographic number range, based on the access code 076, for VoIP-based services. ComReg currently allows VoIP providers to offer both geographic and 076 numbers to end users, regardless of whether the VoIP service is PATS/non-PATS or fixed/nomadic.

In its document 10/60a[24], ComReg has recently suggested various revisions to the version 7 of the National Numbering conventions (NNC). Taken together, it is hoped the following revisions[25] will provide renewed incentives to encourage growth in the use of the 076 numbering range:

- In the case of fixed line operators, a change in the 076 tariff from national call rate to local call rate and a further suggestion of having more than one 076 rate (i.e. a sub-local call rate)
- In the case of mobile originating calls, a requirement for the 076 tariff to be no greater than the rate applied for calls to geographic numbers

We also believe that ComReg is trying to encourage the inclusion of calls to 076 in tariff bundles.

[24] Document 10/60a is a consultation draft – the final version identification will only be known when the consultation period ends.

[25] See 10/60a, Section 10.7.10

ComReg has also suggested amendments to Section 10.7.2 of the National Numbering convention, most notably the extension of the limitation of two numbers per registered user to all undertakings, not just ECS providers. The requirement for ECS providers to undertake reasonable efforts to ensure delivery of emergency calls has also been removed in version 7 of the NNC to reflect the change made to the definition of PATS in the new regulatory framework.

6.2.2 Changes introduced by new regulatory framework

Directive 2009/140/EC introduces a number of comparatively minor amendments to Article 10 (Numbering, naming and addressing), where the use of "assignment" is replaced by "granting of rights of use" in the first two clauses, whilst clause 4 now reads (emphasis added):

> 4. Member States shall support the harmonisation of **specific numbers or numbering ranges** within the Community where it **promotes both the functioning of the internal market** and the development of pan-European services. The Commission may take appropriate technical implementing measures on this matter.
>
> …

6.2.3 Discussion, conclusions and recommendations

The amendments made by Directive 2009/140/EC have no impact on the availability of numbers to VoIP service providers in Ireland. ComReg's allocation of the 076 number range, as well as access to geographic numbers, continues to satisfy an underlying preference for geographic numbers whilst still supporting the evolution of a more flexible perception of numbers. The establishment of the 076 range continues to support a future in which consumers may desire a single contact number that is not associated with a particular type of service, whether fixed, nomadic or mobile.

However, our stakeholder consultation identified a common view within the industry that the success of the 076 numbering range has been rather limited. In general, stakeholders believe this lack of success is attributable to:

- Currently users generally prefer geographic numbers
- The pricing of calls to 076 numbers is prohibitive, compounded by 076 calls not generally being included in call bundles

R18. In conclusion, we believe no specific action is required for numbering regarding VoIP in relation to changes in the Directives. Aspects of existing ComReg policy relating to nomadic use (e.g. 04/103 decision 18) could be restated.

6.3 Access to cross-border numbers and services

6.3.1 Background

Traditionally consumer protection issues in the electronic communications sector have been limited to within the consumer's own Member State borders, and existing enforcement mechanisms reflect this. However, new technology including VoIP means that there is increasing scope for consumers to consume services provided from Member States other than their own. This has already created some new consumer protection challenges for NRAs, and it is expected that cross-border consumer protection challenges will increase as service providers are increasingly able to provide services to consumers outside their own national borders.

6.3.2 Changes introduced by new regulatory framework

One particular example of cross-border service provision is in the area of numbering. Article 28 of the revised Universal Service Directive provides that (subject to some caveats), consumers in one Member State should be able to access any number in the Community. The new Article also anticipates that these consumers may become victims of fraud or misuse (of numbering resources) and empowers NRAs to block access to the numbers in question and to require operators to withhold interconnection revenues.

ComReg 05/50 currently states:

> 4.13 Premium Rated Services
>
> 1. It is a requirement of the Irish National Numbering Conventions that SPs offering on-line services should not provide access by end-users located outside the State to Irish Premium Rate Numbers (i.e. those number ranges commencing '15') unless the SP accepts direct liability for any consequent bad debt that arises as well as liability for any potentially unacceptable content being delivered across borders.
>
> 2. SPs providing access by Irish consumers to Premium Rated Services[26] of non- Irish origins should provide information to their customers about the high charging rates being applied.

[26] Services in this category include (a) services using foreign or international Premium Rate Numbers; (b) equivalent services - in terms of premium pricing and type of content – to Premium Rate Services, but using ordinary numbers with non-Irish country codes.

6.3.3 Discussion, conclusions and recommendations

R19. As Section 4.13 of ComReg 05/50 largely reflects the requirements of Article 28, and noting that ComReg consider there to be no inconsistency in this regard, **we recommend this section should be adopted in future guidelines.**

R20. The ERG began in 2009 to consider the scope of problems associated with cross-border enforcement. During 2010/11, BEREC will continue this work and will focus particularly on the numbering aspect with reference to Article 28. **We recommend that ComReg monitor this work.**

6.4 Number portability

6.4.1 Background

Article 30 of the Universal Service Directive (2002/22/EC) indicates (emphasis added):

> 1. Member States shall ensure that **all subscribers of publicly available telephone services, including mobile services, who so request can retain their number(s) independently of the undertaking providing the service:**
>
> **(a) in the case of geographic numbers, at a specific location;**
>
> **and**
>
> **(b) in the case of non-geographic numbers, at any location.**

In line with Article 30, current Irish legislation and ComReg policy obliges PATS service providers to offer reciprocal number portability to other PATS providers.

An ECS VoIP service provider assigning Irish telephone numbers to customers is obliged to offer number portability to those customers upon request by another ECS VoIP service provider. An ECS VoIP service provider is obliged to offer number portability to customers upon request by individual PATS providers in cases where those PATS providers confirm they are prepared to reciprocate with porting to the ECS VoIP service provider concerned. PATS providers are not obliged to port geographic numbers out to ECS VoIP service providers. 076 numbers are portable between all 076 providers.

If a service provider is unable to offer a number porting facility, this must be clearly stated in all advertising and promotional materials describing the service that are made available to prospective customers in advance of the point of sale and in the service provider's customer service contract.

All number portability transactions with customers and other service providers must be undertaken in accordance with current legal and regulatory rules and guidelines and with industry agreed processes and procedures.

6.4.2 Changes introduced by new regulatory framework

Directive 2009/136/EC introduces the following amendments to Article 30, *Facilitating change of provider* (previously titled *Number portability*) (emphasis added):

---

1. Member States shall ensure that **all subscribers with numbers from the national telephone numbering plan who so request can retain their number(s) independently of the undertaking providing the service** in accordance with the provisions of Part C of Annex I.

…

4. Porting of numbers and their subsequent activation shall be carried out within the shortest possible time. In any case, **subscribers who have concluded an agreement to port a number to a new undertaking shall have that number activated within one working day**.

Without prejudice to the first subparagraph, competent national authorities may establish the global process of porting of numbers, taking into account national provisions on contracts, technical feasibility and the need to maintain continuity of service to the subscriber. **In any event, loss of service during the process of porting shall not exceed one working day**. Competent national authorities shall also take into account, where necessary, measures ensuring that subscribers are protected throughout the switching process and are not switched to another provider against their will.

Member States shall ensure that appropriate sanctions on undertakings are provided for, including an obligation to compensate subscribers in case of delay in porting or abuse of porting by them or on their behalf.

…

6.4.3 Discussion, conclusions and recommendations

According to the 2002 Universal Service Directive, only subscribers of PATS have the right to number portability. However, as number portability is a key facilitator of consumer choice and effective competition it is difficult, from a user's point of view, to justify why a certain kind of services would be excluded from portability. In practice, the changes introduced by the new regulatory framework (in particular, the changing of the definition of PATS and the removal of

"ECS using telephone numbers") mean that it is no longer possible to have "second class" service providers with some limitations on number portability.

However, a more significant implication for the industry as a whole is the change in the time allowed for number portability – operators, both fixed and mobile, must be able to port customer numbers within one working day. Whilst it only takes two hours to port a mobile number in Ireland, we understand the porting of numbers between networks providing service at a fixed location can currently take up to 10 days.

ComReg's number portability requirements for service providers are outlined in draft form in ComReg doc 10/60a Section 10.5, and in various other industry documents. The principal change to the requirements is the conditionality that previously existed in certain circumstances, with respect to the porting of numbers between PATS and ECS providers, has been removed in line with the changes introduced by the new regulatory framework. ComReg has indicated that in practice Irish service providers already respect such arrangements so the change should have no practical impact.

R21. The amendments to Clause 30(1) of the Universal Service Directive also mean that once transposed, **the number portability policy relating to ECS, as previously outlined in the VoIP guidelines (ComReg 05/50), is no longer applicable as number portability obligations now apply to all undertakings providing numbers from the national numbering plan.**

In addition to the changes relating to PATS and ECS providers, the new regulatory framework mandates that all number ports must be completed within one working day. ComReg is currently facilitating an industry Working Group which we understand is making progress on the practicalities of implementing this.

7 Interconnection

7.1 Current position

The ComReg position on interconnection for VoIP purposes means in effect that new interconnection products should be "brought about through commercial negotiation between interested parties". For example, 04/103 says:

> Decision No. 14. For all number ranges other than 076 ComReg will not initiate moves in respect of interconnection, settlement or retention terms for VoIP services but may instead respond, if necessary, to appeals or complaints from VoIP operators if it considers that market development or competition are being impeded or unduly slowed through failure or lack of balance in commercial negotiations.

Special arrangements apply to the 076 range, based on existing arrangements for non-geographic numbers.

If a situation of market failure were to arise, ComReg is obliged if so requested by either party to intervene in order to redress the situation. Likewise, if an undertaking requests intervention, ComReg is obliged to investigate and if necessary intervene.

7.2 Discussion

Nothing in the new directives in our view requires ComReg to alter its current position.

The future of voice interconnection, such as a possible move to Bill and Keep (BAK) and the many associated issues that go with it, are the subject of ongoing work by BEREC, which may have an impact on how this is regulated in the future. We understand that ComReg is continuing to contribute to the BEREC work in this area.

8 Summary of conclusions and recommendations

8.1 Conclusions

The regulatory treatment of VoIP has a complex history. Relevant ComReg documents include:

- A series of decisions related to VoIP services (04/103). These decisions primarily concerned the allocation of numbers to VoIP providers including the opening of a new number range 076.
- Non-binding guidelines for VoIP service providers on the treatment of consumers (Doc 05/50)
- a review of the VoIP regulatory framework (06/45).

Since that time, in 2009, the European Commission has updated the regulatory framework in a number of ways.

In this context, ComReg has commissioned Analysys Mason to conduct a review of the regulation of Voice over Internet Protocol (VoIP) / Voice over Broadband (VoB) in Ireland. Our review has accounted for national developments, as informed by a series of interviews with key stakeholders in Ireland, and the activities of national regulatory authorities (NRAs) across a number of other Member States.

The revisions to the framework cover a number of areas which have specific impact on service providers using VoIP technologies, which we have looked at in turn:

- the security and integrity of networks and services
- access to emergency services, including the ability to make emergency calls, the provision of caller location information, and the level of resilience expected
- The service quality experienced by end users, and the minimum quality of service expected of undertakings' networks
- numbering issues, including the availability of numbers and number portability
- interconnection

8.2 Summary of recommendations

Our recommendations, repeated below, should be understood to be relevant to the period after transposition of the 2009 directives into Irish law.

R1. We recommend that undertakings providing PCNs or PECS should adopt best practice in relation to security and integrity, including the following matters:

- **High level security policy with very clearly defined statements of security requirements - this should include sections covering:**

  - **security governance, risk management and compliance**
  - **asset management and control**
  - **personnel security**
  - **technical information security & assurance controls**
  - **physical security**
  - **business continuity and incident management**
- **At a more detailed level, the following considerations, amongst others, may be appropriate:**
  - **requirements for patch management ensuring that all devices have the appropriate security patches applied within a suitable timeframe**
  - **the use of encryption technologies to encrypt data while in transit, and at rest while stored within applications**
  - **the structuring of networks to achieve the secure separation of data – for example separating VoIP traffic from customer data**
  - **logging and monitoring of security events to enable the detection and investigation of security incidents and breaches**
  - **incident management and reporting procedures, enabling the reporting of incidents to ComReg and the CERT as defined in the National Cyber Security Strategy**
  - **outline procedures for the independent regular auditing and vulnerability scanning of service providers security controls**

Undertakings providing PCNs or PECS should provide an annual report to ComReg documenting the approach they are taking to meeting their obligations to ensure security and integrity of their networks and services. They should also report to ComReg any significant changes to their ability to ensure security and integrity of their networks and services in a timely manner.

We note that standards for network security and integrity are under development at a European level and that it is expected that operators will monitor these developments and implement systems meeting the required standards within a reasonable period, once these European standards are finalised.

R2. **We recommend that all voice providers note their need to comply with the new regulatory framework, and meet their obligations with respect to "force majeure". Best practice to support this may include, for example, risk mitigation strategies geared towards ensuring critical points are serviced by adequate:**

  - **redundancy,**
  - **diversity,**
  - **and recovery capability**

Consideration of acceptable levels of "mean time to repair" (MTTR) may also be appropriate, as well as consideration of business continuity and disaster recovery plans.

R3. For reasons of practicality, **we recommend that ComReg allow service providers a reasonable period to introduce the measures necessary to meet their obligations. Improvements to policies and procedures may be achievable within a relatively short period, but the introduction of network changes to improve network security, integrity and resilience will be subject to design, procurement and implementation timescales and in some cases commercial agreement with other service providers. For these reasons we recommend that ComReg allow service providers at least 12 months to introduce all necessary measures.**

R4. **ComReg should withdraw their existing access to emergency calls policy relating to ECS providers, as outlined in the VoIP guidelines (ComReg 05/50), as the obligation to provide access to emergency services now applies to all undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan.**

R5. We recommend that the competent authority should link the accuracy and reliability requirements to the ECAS specification. For example, "all fixed location PATS providers which are not nomadic providers shall provide Fixed Line Location Information to the ECAS in accordance with the ECAS RIO/LIRO, and the key local specifications referenced by the ECAS RIO". This may need to be enhanced with requirements concerning the reliability of the information.

R6. Furthermore, we recommend that a provider of PATS at a fixed location should obtain (from the customer if necessary) the physical location at which the service will normally be used before they activate a new customer's service.

R7. We recommend that providers of PATS at a fixed location should also provide one or more easy ways for their customers to update the physical location they have registered with the provider (e.g. via a secure Internet service), if it changes.

R8/9. We recommend that:

- **In the short term, where it is not technically feasible for an undertaking to provide accurate caller location information because it is VoIP originated, ComReg should allow undertakings to present these calls to the ECAS.** We note that the ECAS schedule 5 obliges the operator to provide to the ECAS provider an indicator that the call is a VoIP Originated Emergency Call.
- **In the medium term, ComReg should monitor developments in Europe and internationally and may wish to commence discussions with the DCENR in relation to the development of a national architecture, which may be similar to those developed by the NENA and NICC, for providing sufficient location information of nomadic VoIP users to the ECAS. This work could be guided by the EENA NG112 TC, and will need to accommodate the use of traditional networks and the future migration to end-to-end IP connectivity.**

R10. We recommend that until such time that a national solution for providing sufficient location information for nomadic users to the ECAS is in place, end-users of nomadic services should be clearly informed that nomadic use of their VoIP service may not influence where a call to the emergency services is directed, i.e. the call will most likely be directed to their "home" emergency services, rather than to the emergency services appropriate to their current location.

R11. On the basis of Recital 40, **we recommend that undertakings take the "necessary measures" needed to ensure service availability and uninterrupted access to emergency services**.

R12. We recommend that service availability should be equal to that provided by broadly similar categories of voice provider:

- **voice services provided by a wired access provider should meet an availability standard equivalent to the existing PSTN. Should battery backup be required for CPE, or for remote infrastructure, the time supported by the batteries should be sufficient to cover either the great majority of repairs or end users should be warned that an alternative means of calling may need to be employed.**
- **voice services provided by wireless access providers should meet an availability standard at least equivalent to the best of existing cellular networks**
- **voice services provided by a network independent provider should seek to meet an availability level as high as is feasible given their lack of control over certain parts of the infrastructure used to provide the service. We note that these providers would be expected to make use of all appropriate techniques such as**
  - **prioritization**
  - **negotiation of suitable service level agreements.**

For the avoidance of doubt, it is not envisaged that the current level of availability will be reduced.

R13. **We recommend service providers should inform their customers clearly of any ways in which the emergency calls service may not be fully equivalent to the traditional wireline PSTN. Customers should be informed in any guide issued by the service provider, and the same information should be included in materials made available to prospective customers in advance of the point of sale.**

R14. To understand whether there are specific service quality issues which may make the new clause 22(3) more pertinent, we recommend that **one input which ComReg could consider before taking any further action is the volume of customer complaint data. This, amongst other considerations, may indicate whether there is a need for ComReg to set any specific**

quality of service requirements on undertakings providing voice services using specific technologies, such as VoIP.

R15. As the provisions on contracts, information transparency and quality of service apply to all providers of communications networks or services, not only VoIP service providers, we recommend that in the first instance **action might be necessary to remind all providers of their duties once the 2009 Framework is transposed**.

R16. We recommend that **undertakings should be encouraged to provide terms and conditions in plain English.**

R17. As regards network neutrality we recommend that ComReg continue to monitor the market situation, but at this point we consider that no action need be taken by ComReg as the BEREC work is likely to generate a harmonised position at EU-level. Intervention should only be necessary in the case of critical failure.

R18. We believe no specific action is required for numbering regarding VoIP in relation to changes in the Directives. Aspects of existing ComReg policy relating to nomadic use (e.g. 04/103 decision 18) could be restated.

R19. As Section 4.13 of ComReg 05/50 largely reflects the requirements of Article 28, and noting that ComReg consider there to be no inconsistency in this regard, **we recommend this section should be adopted in future guidelines.**

R20. The ERG began in 2009 to consider the scope of problems associated with cross-border enforcement. During 2010/11, BEREC will continue this work and will focus particularly on the numbering aspect with reference to Article 28. **We recommend that ComReg monitor this work.**

R21. We note that the amendments to Clause 30(1) of the Universal Service Directive also mean that once transposed, **the number portability policy relating to ECS, as previously outlined in the VoIP guidelines (ComReg 05/50), is no longer applicable as number portability obligations now apply to all undertakings providing numbers from the national numbering plan.**

Annex A: Historical regulation of VoIP

A.1 Overview

Since the introduction of the European regulatory framework in 2002, the regulation of VoIP has been studied extensively by the European Commission (in 2004 and again in 2008), the European Regulators Group (ERG) (in 2005 and 2007), and by various National Regulatory Authorities (NRAs).

Detailed views on the regulation have changed over time, along with the market and the technology. Nonetheless, there are common threads. Many common themes, including numbering and emergency services, visible in the earliest assessments, are carried through to the new regulatory framework.

A.1.1 Rights and obligations under European regulatory framework (2002)

As defined in the Framework Directive (2002/21/EC) and the Universal Service Directive (2002/22/EC), a provider of voice services may belong to one or more of the following categories:

- A provider of a publicly available electronic communications service (ECS);
- A provider of a publicly available telephone service (PATS);
- A provider of a PATS service pursuant to a universal service obligation;

Operators choosing to enter the market as a provider of publicly available ECS are associated with a number of obligations and rights under the regulatory framework agreed in 2002, as shown in Figure A.1.

Obligations for ECS providers	*Rights for ECS providers*
Notification of the NRA (Authorisation Directive, Article 3(2))	Right to provide an ECN or ECS (Authorisation Directive, Articles 3 and 4)
Financing of Universal Service Obligations (Universal Service Directive, Article 13)	Consideration of application to use public rights of way (Authorisation Directive, Article 4; Framework Directive, Article 11)
Obligation to make contracts available to end users (Universal Service Directive, Article 20)	Right to negotiate interconnection (Authorisation Directive, Article 4(2), Access Directive, Articles 3 and 4)
Possible obligations to publish information on the quality of their services (Universal Service Directive, Article 22)	Right to use telephone numbers (Framework Directive, Article 10; Authorisation Directive, Article 5)
Make available the relevant information for the provision of publicly available directory enquiry services and directories (Universal Service Directive, Article 25(2))	Right to apply for the right to offer Universal Service (Authorisation Directive, Article 4(2), Universal Service Directive, Article 8(2))
Provision of access to directory enquiry and operator assistance services (Universal Service Directive, Article 25(3))	
Conditions attached to use of numbers (Authorisation Directive, Annex C)	
The user has the right to place calls to non-geographic numbers where technically and economically feasible (Universal Service Directive, Article 28)	
Safeguard security of its services (Directive on privacy and electronic communications, Article 4)	
Privacy obligations (Directive on privacy and electronic communications, Articles 5, 6, 7 and 9)	

Figure A.1: Rights and obligations for ECS providers under 2002 framework [Source: EC / OJEU]

In the 2002 Framework, operators providing PATS have a number of additional rights and obligations over and above the obligations and rights listed above for publicly available ECS. These rights and obligations are listed in Figure A.2.

Obligations for PATS operators	*Rights for PATS operators and subscribers*
Obligation to provide access to emergency services (Universal Service Directive, Article 26(1))	Right to Carrier Selection and Pre-selection on the network of an SMP operator (Universal Service Directive, Article 19)
Obligation to implement number portability (Universal Service Directive, Article 30(1), 30(2))	The subscriber to PATS has a right to exercise Number Portability (Universal Service Directive, Article 30(1))
Ensure uninterrupted access to emergency services (Universal Service Directive, Article 23)	The subscriber to PATS has the right to appear in a publicly available directory (Universal Service Directive, Article 25(1))
Transparency and publication of information (Universal Service Directive, Article 21)	
Obligation to realise entry in the directory if requested (Universal Service Directive, Article 25(1), Directive on privacy and electronic communications, Article 12)	

Figure A.2: Rights and obligations for PATS providers under 2002 framework [Source: EC / OJEU]

The 2002 Framework Directive defines Electronic Communications Service (ECS) as:

- a service normally provided for remuneration
- which consist wholly or mainly in the conveyance of signals on electronic communications networks[27]

The Universal Service Directive defines Publicly Available Telephone Service (PATS) as a service

- available to the public
- for originating and receiving national and international calls and
- access to emergency services
- through a number or numbers in a national or international telephone numbering plan[28]

The net effect of this patchwork of rights and obligations, combined with the definition of PATS, is that VoIP providers can be in one of four categories:

- Not an ECS if they do not use telephone numbers
- An ECS, using telephone numbers
- PATS, if they provide access to the emergency services
- PATS and USO provider, if they provide access to the emergency services and are designated as USO provider.

[27] See Directive 2002/21/EC, Art. 2(c)

[28] Directive 2002/22/EC, Art. 2 (c).

A.1.2 ERG common position

In 2007 ERG adopted a Common Position[29] (CP) on the regulation of VoIP, replacing the Common Statement of 2005[30]. The CP made a comprehensive analysis of ex-ante regulation applied to VoIP services and set out a number of recommendations, many of which are reflected in the new regulatory framework, focused on the following areas:

- Access to emergency services
- Numbering
- Number portability
- Consumer rights and service provider obligations
- Definitions of ECS / PATS / Public Telephone Network (PTN)

The ERG VoIP Action Plan[31], based on responses from 28 NRAs in the European Economic Area plus BAKOM (Switzerland), recorded the then current state of implementation of the action programme set out in the CP - assessing the current state of conformity and identifying where further changes are in train or under review.

A.1.3 European Commission review proposals (2007)

The issues that are relevant in this report were also considered as part of the Commission's overall review of the European regulatory framework:

- The lack of common numbering arrangements in the Member States
- The classification of PATS in the 2002 Universal Service Directive
- Access to emergency services
- Caller location information
- Number portability

[29] ERG Common Position on VoIP, ERG (07) 56rev2, December 2007

[30] ERG Common Statement for VoIP regulatory approaches, ERG (05) 12

[31] VoIP Action Plan – to achieve conformity with ERG common position, ERG (09) 19, June 2009

A.1.4 European Commission study (2008)

In 2008, WIK-Consult GmbH, in conjunction with Cullen International, conducted a study of the regulation of VoIP on behalf of the European Commission. The study made a number of recommendations relevant to this report:

- **Access to numbers:** Bureaucratic hurdles to obtaining numbers need to be reduced if not eliminated. The duration for a response to a request for numbers should not exceed the levels specified in Articles 4 and 5 of the Authorisation Directive, and effective recourse must be available to the ECS provider.

- **Geographic versus non**-geographic **numbers:** Numbering plans should be technologically neutral. Geographical numbers for traditional telephony services and geographical numbers for VoIP services (including nomadic services) should share the same number range.

- **Emergency services:** The Commission should require Member States to ensure that any providers of a service available to the public for originating national calls through a number or numbers in a national telephone numbering plan provide access to emergency services. Such providers should also be required to make caller location information available to authorities handling emergencies, to the extent technically feasible. Reasonable transition periods should be allowed. Such providers should be obliged to clearly inform subscribers about any limitations in the access to emergency services they offer, as compared to that offered by the traditional telephony service. To the extent that location determination depends on the subscriber's own actions, it is crucial that the subscriber be educated and informed as to the obligations that he or she must undertake to keep this location information current.

  The Commission (with the ongoing support of the European Regulators' Group (ERG) and the Expert Group on Emergency Access (EGEA)) should continue to monitor developments as regards technical standards and actual deployment in regard to VoIP access to emergency services. In particular, at such time as a deployment of enhanced Public Safety Access Points (PSAPs) is ripe (especially a migration of the PSAPs to IP), some level of European coordination will be necessary and appropriate.

A.1.5 ComReg review of VoIP regulatory framework (2006)

In 2004, ComReg issued a series of decisions related to VoIP services (04/103). These decisions primarily concerned the allocation of numbers to VoIP providers including the opening of a new number range 076. In July 2005, ComReg issued non-binding guidelines for VoIP service providers on the treatment of consumers (Doc 05/50) and, in August 2006, ComReg published a review of the VoIP regulatory framework (06/45). The positions adopted by ComReg in its review of the Irish framework are summarised in Figure A.3.

Decision Notice Issue	*ComReg Position (ComReg 06/45)*
Geographic numbering	Rules surrounding use of geographic numbers considered sufficiently liberal to allow VoIP service providers to develop and offer services on a par with those service providers offering PSTN-based services
076 number range	Current interconnection settlement regime facilitates VoIP service providers to launch competing services using the 076 number range
Provision of voice services and associated obligations	Service providers expected to place a prominent link to VoIP guidelines (Doc 05/50) on their website. VoIP service providers must ensure that ECS/PATS classification of their services notified to ComReg is correct and re-notify if necessary
Access to emergency services	Service providers who offer a service classified as PATS must offer guaranteed, free-of-charge access to emergency service numbers 112 and 999. Service providers who offer services classified as ECS, and that use numbers, must ensure customers are advised of any limitations of their services, including, but not limited to, the provision of guaranteed access to the emergency services
Number portability	Service providers offering services classified as PATS must offer number portability, regardless of number type. This is also a right of these service providers, as number portability works on a reciprocal basis. All service providers offering service that use a number from the 076 range must also support number portability. All those providers offering services classified as ECS using geographic or non-geographic numbers (apart from numbers from the 076 range) must offer number portability to a PATS provider, once it is offered on a reciprocal basis
Calling line identification (CLI)	CLI should only be provided if its veracity can be guaranteed. If this cannot be guaranteed then CLI must be set to “Unavailable”
Access to directory enquiry services and directory listings	Customers of those services classified as PATS must be able to have their number listed in the National Directory Database (NDD), should they so choose, as well as providing access to directory enquiry and operator assistance services. Services classified as ECS not obliged to offer these facilities, but ComReg encourages ECS providers to offer some or all of these facilities.
Quality of Service (QoS) and network integrity	VoIP guidelines (Doc 05/50) set out how service providers of VoIP services should inform their customers of the limitations of their service vis-à-vis what customers might legitimately expect compared to a PSTN-centric network
Port blocking and service degradation	Marketplace ought to be allowed to deal with any such issues should they arise. ComReg reserves the right to intervene should such an approach prove to be ineffectual
Interconnection	Any new VoIP interconnection product should be brought about through commercial negotiation between interested parties. If a situation of market failure were to arise, ComReg is obliged to intervene to redress the situation

Figure A.3: ComReg positions – Result of VoIP framework review (August 2006) [Source: ComReg]

A.2 Security and integrity of networks and services

Requirements under European regulatory framework (2002)

The 2002 framework sets out a variety of requirements with respect to the security and integrity of networks and services:

- In the context of access to emergency services (Article 23 of the USD), the importance of service availability and reliability is specifically mentioned. Article 23 (Integrity of the network) requires that:

> Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations. Member States shall ensure that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

- There is a requirement to take appropriate measures to safeguard security of services and to notify users of potential breaches of security. The e-privacy directive recital 20 says:

> (20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. ...

- This is formalised in e-privacy Directive Articles 4 and 5

Article 4 Security

1 The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5 Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality. …

- General conditions of authorisation are permitted to contain requirements relating to Security of public networks against unauthorised access according to Directive 97/66/EC.

Annex B: Caller location architectures

B.1 General

The standardisation community has over the last few years worked on a number of architectures designed to better automate the determination of location. ECRIT (Emergency Context Resolution with Internet Technologies) is the IETF's initiative to develop an overall protocol architecture to enable VoIP (and other IP-based services) to access emergency services, whilst in the US the National Emergency Number Association (NENA) has developed its i2 architecture[32] to support the interconnection of VoIP domains with the existing Emergency Services Network infrastructure in support of the migration toward end-to-end emergency calling over the VoIP networks between callers and PSAPs. The differences between the i2 specification and the newer i3 specification are largely based on the assumptions being made about the capabilities of the infrastructure available to the PSAP operator. For i2, the PSAP operator receives emergency calls via the PSTN and for i3 the PSAP operator operators an IP-based emergency services network.

Groups in different countries, typically led by the PSAP operator community, have also started to investigate on how to integrate VoIP emergency calls into their existing infrastructure. As an example, the activities provided by the Network Interoperability Consultative Committee (NICC) in the UK fit into this category[33].

Whilst the NICC did not use the NENA i2 architecture as their starting point, similarities did arise and, where possible, the names of i2 interfaces have now been re-used and modified within the NICC specification with the aim of being useful when international scenarios are considered in future. The NICC work to this point focuses on the (majority) case where all parties are in the UK and ADSL access is used. Their Location Information Working Group is now beginning to examine other "use cases" of the architecture, for example usage within enterprise IP networks and also cable access networks.

To avoid highly customised solutions within each Member State of the EU, a technical group within the European Emergency Number Association (EENA) has also been formed to synchronise various activities by considering the country-specific circumstances regarding their current emergency infrastructure. The EENA Next Generation 112 Technical Committee (NG112 TC), is chaired by Hannes Tschofenig (former Chair of IETF-ECRIT) and vice-chaired by Roger Hixson (NENA Technical Issues Director).

---

[32] NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2), August 2010 (http://www.nena.org/sites/default/files/20100811_08-001%20v2.pdf). This issue of the i2 standard supports E911 for fixed and nomadic VoIP services. Support for mobile VoIP services will be covered in a future release.

[33] VOIP - Location for Emergency Calls (Architecture) - NICC ND 1638 Issue 1.1.2 (2010-3)

B.2 Overview of NENA i2 architecture

Figure B.1 shows a simplified overview of the i2 architecture, highlighting the main functional elements used to support validation and management of location information.

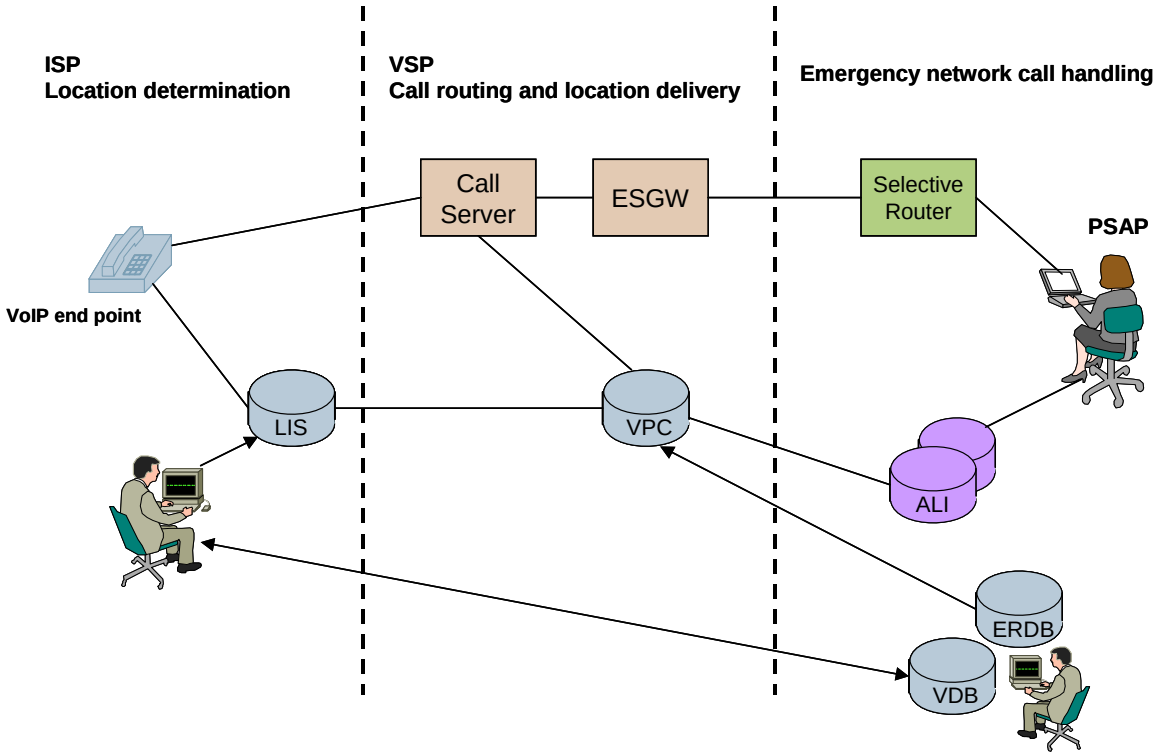

Figure B.1: Simplified overview of the i2 architecture [Source: NENA / Analysys Mason]

The Call Server is the entity in a private or public IP domain that provides service to endpoints in an emergency caller's home domain. The Call Server may use SIP or some other VoIP signalling protocol.

The Emergency Services Gateway (ESGW) is the signalling and media inter-working point between the IP domain and conventional trunks to the 112/999 Selective Router. The Selective Router delivers calls arriving on trunks from the ESGW to the correct serving PSAP based on the routing information in the call setup signalling.

The Location Information Server (LIS) is the functional entity that provides locations of endpoints. A LIS can provide location-by-reference, or location-by-value, and, if the latter, in geo or civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID or Media Access Control (MAC) address, and returns the location (value or reference) associated with that identifier. The administrator/owner of

the LIS, the ISP in this simplified overview, is responsible for creating and maintaining this mapping.

The VoIP Positioning Centre (VPC) is the element that provides routing information to support the routing of VoIP emergency calls. It also cooperates in delivering location information to the PSAP using the existing Automatic Location Identification (ALI) database infrastructure.

The Emergency Service Routing Zone Database (ERDB) contains the routing information associated with Emergency Service Zones (ESZs). It supports the boundary definitions for ESZs and the mapping of civic address or geo-spatial coordinate location information to a particular ESZ. When an emergency call is originated and location information is received from the VPC, the ERDB will identify the ESZ and routing information associated with the location information.

The Validation Data Base (VDB) contains information that describes the current, valid civic address space defined by the Emergency Services Network Provider. The VDB will return a response indicating that a given location is a valid address or an error response. This process ensures that the address is a real address (i.e. the address exists) but does not ensure that it is the location of the caller.