Privacy in Electronic Communications: The Regulation of VoIP in the EU and the United States

DANIEL B. GARRIE* AND REBECCA WONG**

LT Voice over Internet Protocol; Privacy; Internet telephony; Data Protection Directive 95/46; Directive on Privacy and Electronic Communications 2002/58; Wiretap Act 18 USC §2510 (12).

Introduction

The growth of internet telephony or Voice over Internet Protocol (VoIP) services has led to questions by policymakers and legislators over the regulation of VoIP. In this article, the authors consider the extent to which VoIP services are protected from an EU/US perspective and the concerns arising from the current legislative framework, mainly from privacy perspective. The second part considers VoIP services in general. The third part examines the European framework and in particular, the current categorisation of VoIP services, before considering the privacy perspective, taking into account the Directive on Privacy and Electronic Communications 2002/58 and the general Data Protection Directive 95/46. The fourth part will consider the US framework in protecting the privacy of communications, asserting that the federal courts and legislatures should act to explicitly protect VoIP oral internet communications. The final part will conclude by discussing the principal areas that still need to be addressed.

What is VoIP?

In its broadest definition, VoIP can be described as the ''conveyance of voice, fax and unrelated services publicly or wholly over packet switched IP-based networks including peer-to-peer VoIP and VoIP services connected to PSTN''.[1] This section presents a broad overview of the technology involved in both internet voice and data transactions. It discusses, in a non-technical manner, how VoIP transmits voice communications over the internet.

VoIP is a technology by which oral communications can be transferred from circuit-switched networks to or over Internet Protocol networks, and vice versa. VoIP transforms standard oral telephone signals into compressed data packets that are sent over the Internet Protocol. The audio signal at this point is captured either by way of a microphone or received from line input. This analogue representation is then converted to a digital representation at the audio input device. The resulting digital samples are copied into a memory buffer in blocks of frame length. Here, a silence detector decides whether the block is silence or a portion of speech. Prior to transmission over the internet, the block itself is written to a socket. Once this is completed, the communication is transmitted to another VoIP terminal. This terminal parses the header information and the block of audio is decoded applying the same codec and the samples written into a buffer. Once this step is complete, the block of samples is copied from the buffer to the audio output device. The audio output device makes the digital to analogue conversion and outputs the signal. VoIP can be used with either a telephone or a PC as the user terminal. This gives different modes of operation: PC to PC, PC to telephone, telephone to PC and telephone to telephone (via the internet), all VoIP protocols are application layer protocols.

People have been aware of the potential for wiretapping, but the public perceives such actions to be limited to corporate espionage and criminal activities.[2] To eavesdrop over the switched telephone network there must be physical access to the telephone line and access to some type of hardware device that may or may not be very sophisticated.[3] The equipment or software needed is much more sophisticated, but well

* Daniel B. Garrie, Esq., is Managing Director at the venture capital firm EMI Capital LLC and a court-appointed e-discovery neutral via Alternative Resolution Centers (ARC). Grateful acknowledgments to: Stuart A. Garrie; Stephen J. Williams, Sarah E. Haines, Michael D. Garrie, Nicole L. Garrie, Erica V. Garrie to whom the author owes a great deal of his success.

** Dr Rebecca Wong is Senior Lecturer in Law, Nottingham Law School, Nottingham Trent University, UK.

1 OECD, Working Party on Telecommunications and Information Services Policies: policy considerations of VOIP, at *http://www.oecd.org/dataoecd/59/55/36316212.pdf* [Accessed June 11, 2009].

2 J Fitzgerald, ''Team to Tie Net Phone Hackers; Industry Aims to Stop Scams before they Start'', *Boston Herald*, April 26, 2005, p.31.

3 VoIP is a solid technology; however, it requires government regulation to ensure a certain level of product reliability and safety for the consumer. Y. Nishiyama, ''Vulnerabilities in Electronic Commerce Communication: IM & VoIP'', World Bank, Washington D.C. (2003). Up until today security issues in the data and voice worlds have been seen to be completely separate by the users. With the advent of VoIP, users are now exposed to the risks of sending data over the internet while simultaneously having the expectation that telephone conversations are between the parties involved. VoIP is vulnerable because convergent technologies lead to weakness from multiple points. In addition, VoIP must address the security holes in cell-phones that arise from the transport mechanisms used when mobile phones are in use. Adjoining these problems is the reality that cell tracker tools have evolved and people can eavesdrop with much greater ease on cellular transmission. Also, hackers can intercept data with greater ease then before when the data travels in soft zones (unprotected) between legitimate users and cell towers. Martius Miettinen, ''IT-Security in the Automobile Domain'', Lehrstuhl für Kommunikationssicherheit, Ruhr University at Bochum (Germany), at *http://www.cs.helsinki.fi/u/mjmietti/seminaariS03/automobilesecurity.pdf* [Accessed June 11, 2009]. Thus transmitting information in digital form raises new vulnerabilities, and a digital device can be used either for fiscal or and privacy violations. Also, the VoIP systems run on vulnerable software, so the systems must contend with all of these possible holes.

within the reach of a 16-year-old hacker that has access to e-Bay or the Web. Data sniffing tools are readily available and these tools will soon be enhanced to become aware of the new VoIP protocols broadening access the accessibility to wiretapping tools.[4] Data sniffing tools are used primarily to steal or transmit end-user data from end-users' machines with or without their knowledge.[5] While in an office environment VoIP traffic travels over a data network that is used by all of the regular users of the corporate Local Area Network (LAN), any or all of the conversations traversing a network could theoretically be compromised by anyone with a regular connection on the network.[6] Consequently, VoIP packets could be identified and stored for re-assembly to be played back at a later time.[7] The idea that only internet traffic is at risk is simply wrong.[8] Privacy for oral traffic could be vastly enhanced by the use of encryption.[9]

European framework for the protection of VoIP services

New regulatory framework

At a European level, the protection of VoIP services is broadly covered under the new regulatory framework (NRF) for electronic communications, which was adopted in April 2002 and came into effect on July 2003. The NRF was introduced after a Commission's Communication review back in 1999,[10] which was principally concerned with reforming the telecommunications sector.

The NRF comprises five Directives: the Framework Directive 2002/21[11]; Authorisation Directive 2002/20[12]; Access and Interconnection Directive 2002/19[13]; Universal Service Directive 2002/22[14]; and the Directive on Privacy and Electronic Communications 2002/58.[15] The Framework Directive sets out the main principles and objectives underpinning the EU regulatory policy on the provision of electronic communications services and networks, including the role of the National Regulatory Authority (NRA). The Access and Interconnection Directive deals with the harmonisation of the linking of networks between operators of public communications services.

The Universal Services Directive is important because it principally deals with minimum set of services to be made available to end-users including PATS services (described below); network integrity, directory inquiry services; public payphones; and special measures for disabled users.[16]

The Authorisation Directive establishes a legal framework for Member States on general authorisation[17] and applies to the authorisation of all public and private electronic communications networks[18] and electronic communications services[19] (art.1(2)). By covering all electronic communications networks and services whether provided public or not, the Directive applies to both categories providers so that they can benefit from ''objective, transparent, non-discriminatory and proportionate rights, conditions and procedures'' (Recital 4).

In a report dated 2004,[20] the authors took the view that the following issues needed to be addressed. These were the current categorisation of VoIP as PATS; location independence; emergency access; and network integrity. Given the scope of this article, the discussion will centre on the current categorisation of VoIP from a US and European perspective.

Classification of VoIP providers

In brief, the regulation of VoIP in Europe is slightly complex[21] because there is no consensus over the categorisation of VoIP

4 J. Daniels, ''Scumware.biz Educates About Dangers of Adware/Scumware'' (2004) 5 *Computer Security Update* 2.

5 P.J. Bruening and M. Stephen, ''Spyware: Technologies, Issues, and Policy Proposals'' (2004) 7(9) J. Internet L. 3. Advertisers can use these tools to identify what sites end-users have visited and deliver targeted ads to the end-user's computer. For example, if a user visits a Florida cruise site followed by a later visit to a golfing site, advertising using data sniffing tools will serve advertisements to the end-user's computer about golf course vacations in Florida. Data sniffing tools encompass cookie technology such as Spyware, adware.

6 D.J. Long, ''The Lazy Person's Guide to Voice Telephony—Part II'' (Spring 2004) CHIPS 43. Furthermore, with the onset of widespread adoption of wireless technologies, attempts to intercept communications are likely to grow.

7 A.J. Singer, ''Debate over Voice-Over Internet Protocol Benefits: Cost-Effectiveness, Security Concerns at Heart of Uncertainty'', *San Diego Business Journal*, Vol.51, December 17, 2001.

8 I. Shepherd, ''VoIP: The Maturity of Internet Telephony Technology Opens up Network Safety Concerns Voice over IP: Finding a Balance between Flexible Access and Risk of External Attack'', *Computer Weekly* (Networks 34), April 19, 2005.

9 P. Bednarz (President and CEO, Netergy Microelectronics Inc., Santa Clara, Calif.), Communications Design Conference, ''Security Considerations at Forefront of VoIP Design'', *Electronic Engineering Times*, September 23, 2002, p.63 (adding word encryption and decryption are CPU intensive and take time. If the overall latency of a VoIP call is greater than approximately 250 milliseconds, the quality of the call will noticeably be affected).

10 Commission Communication towards a new framework for Electronic Communications infrastructure and associated services: 1999 Communications Review, COM(1999) 539, November 10, 1999.

11 Directive 2002/21 on a common regulatory framework for electronic communications networks and services [2002] OJ L108/33.

12 Directive 2002/20 on the authorization of electronic communications networks and services [2002] OJ L108/21.

13 Directive 2002/19 on access to, and interconnection of, electronic communications networks and associated facilities [2002] OJ L108/7.

14 Directive 2002/22 on universal service and users' rights relating to electronic communications networks and services [2002] OJ L108/7.

15 Directive 2002/58 concerning the protection of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.

16 European• Commission, Universal Service, at *http://europa.eu* [Accessed June 11, 2009].

17 European Commission, Regulating market access, at *http://europa.eu* [Accessed June 11, 2009].

18 ''Electronic communications networks'' are defined under art..2(a) of the Framework Directive 2002/21 as those ''transmission systems, and where applicable switching and routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the information they convey''.

19 The definition of ''electronic communications services'' is provided under the Framework Directive 2002/21. The definition is covered above in the article.

20 European Commission, IP voice and associated convergent voices, at *http://europa.eu* [Accessed June 11, 2009].

21 D. Bach and J. Sallet., ''The challenges of classification: emerging VOIP regulation in Europe and the United States'', First Monday, at *http://www.firstmonday.org/issues/issue10_7/bach/* [Accessed June 11, 2009].

AQ1

services. The Commission takes a ''light touch'' approach to VoIP regulation. Whether VoIP service is regulated would depend on whether a VoIP service is considered as an electronic communication service (ECS) or a publicly available telecommunications service (PATS).

An ECS is defined under art.2(c) of the Framework Directive[22] as a ''service normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electronic communications networks''. Therefore a VoIP service that provided a product such as a software program to be run on personal computer with no ongoing provision of service would fall outside the scope of the EU regulatory framework.[23]

PATS or not?

A PATS is defined under art.2(c) of the Universal Services Directive[24] 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''.

The classification of a VoIP provider as PATS means that the criteria laid down under the Universal Services Directive would apply. However, not all VoIP providers would be classified as PATS because some providers may not give access to emergency services as required under the definition. Therefore the categorisation of VoIP providers as PATS is not wholly conclusive. In response to a consultation paper on the treatment of Voice over Internet Protocol[25] by the European Commission, the EuroISPA[26] made known their view the need for legal certainty regarding the rights and obligation of the VoIP service providers. In particular, they added that VoIP providers should not be classed as a PATS provider on the basis of certain technical parameters. They took the view that a VoIP provider should be categorised as a PATS provider if its service was accessed from the demand side (i.e. the customer) as a direct substitute for their traditional voice telephony service. Arguably, the demand for VoIP services has not reached the point where it has replaced the traditional telephony service,[27] but the lack of legal certainty in this area does raise significant questions about the extent to which VoIP providers should provide access to emergency services and the like. In a recent decision by the Finnish Communications Regulatory Authority,[28] Ficora held that TeliaSonera VoIP (Sonera Puhekaista) service should be classified as a PATS service on the basis that it was available to the public; users originate and receive national and international calls; there was access to emergency services and the service was available through the Finnish numbering plan. The TeliaSonera's VoIP Service was offered only to their broadband users and was offered as a substitute for PSTN connection. The implications arising from Ficora's decision was that the TeliaSonera VoIP Service had to comply with the obligations set for PATS laid down under the Finnish regulations which included making available to their users, access to the international calls using the access code 00; availability by users to access the emergency call number 112 and other special emergency number free of charge; call barring service at the request of the user free of charge and the provision of itemised bills free of charge to the user.

Ofcom, the United Kingdom's NRA, has used the same criterion as the Universal Services Directive by holding the view that a provider qualifies as PATS if *all* the following criteria were satisfied. Namely, a provider would need to show that it was a service available to the public; for originating and receiving national and international calls and provided access to emergency services through a number or numbers in a national or international telephone numbering plan.[29] What this means is that a VoIP provider based in the United Kingdom, which does not meet all the criteria described above would *not* be considered as PATS.

While it is clear what the criterion is to qualify as PATS, it is unclear what the obligations are for VoIP providers that do not qualify as PATS status. Certainly, non-PATS providers such as peer-to-peer VoIP providers would not have to fulfil the obligations as required under the Universal Services Directive; however, some VoIP providers may constitute an ECS as defined under the Framework Directive or the equivalent national legislation and therefore will be required to comply with the obligations laid down under the NRF.

More specifically, a provider would have to adhere to the Authorisation Directive because it applies to ECS and the Directive on Privacy and Electronic Communications 2002/58 (DPEC), the latter protects the privacy of communications in the electronic communications sector. The DPEC replaces the Telecommunications Directive 97/66 by dealing with the processing of personal data in the context of the electronic communications sector. It complements the general Data Protection Directive 95/46 (which regulates the processing of personal data for non-public communications) by dealing with the regulation of personal data in the context of the electronic communications sector. For a VoIP provider, they would, as with any other organisation or individual that collected personal information, be required to adhere with the general Data Protection Directive 95/46 (DPD) or corresponding national legislation. The Data Protection Directive was passed to harmonise the data protection laws within the European Union[30] and imposes certain obligations on organisations or individuals (''data controllers''[31]) that

22 Directive 2002/21 on a common regulatory framework for electronic communications networks and services [2002] OJ L108/33.

23 Commission Staff Working Document, ''The treatment of Voice over Internet Protocol under the EU Regulatory Framework, at *http://europa.eu* [Accessed June 11, 2009].

24 Directive 2002/22 on universal service and users' rights relating to electronic communications networks and services [2002] OJ L108/7.

25 Commission Staff Working Document, ''The treatment of Voice over Internet Protocol under the EU Regulatory Framework'', at *http://europa.eu* [Accessed June 11, 2009].

26 EuroISPA. DG INFSO Information and Consultation Document: The Treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework: response from the EuroISPA, at *http://europa.eu* [Accessed June 11, 2009].

27 In the last presentation by Mattila on VoIP market trends, it was estimated in September 2003 that there were less than 200,000 VoIP users worldwide whilst there were less than 20,000 VoIP users in Europe. However, the growing number of broadband internet access is likely to accelerate the use of VoIP services. O. Mattila, ''Voice over IP (VoIP)—background and regulatory aspects'', at *http://erg.eu.int/doc/publications/consult_accounting_sep/erg_0422_voip_discussion_note.ppt* [Accessed June 11, 2009].

28 Ficora, Decision of the Finnish Communications Regulatory Authority on compliance with law of the Sonera Puhekaista Service, at *http://www.ficora.fi/englanti/document/SoneraPuhekaista.pdf*.

29 Ofcom, ''Regulation of VoIP Services'', at *http://www.ofcom.org.uk/consult/condocs/voipregulation/voipregulation.pdf* [Accessed June 11, 2009].

30 For a background history into data protection laws in Europe, see L.A. Bygrave, *Data protection law: approaching its rationale, logic and limits* (The Hague: Kluwer, 2002).

31 Data controllers are defined under art.2(d) of the DPD as the ''natural or legal person, public authority, agency or any other body

AQ2

process personal information to comply with the data protection principles as laid down under art.6 of the DPD and corresponding national laws.[32]

Individuals whose personal information is collected by the data controllers are entitled to have a right to know what information is held about them, including information on the purposes of such processing and recipients or categories of recipients of such data (art.10 of the DPD). Furthermore, data controllers are required to implement appropriate technical and organisational measures to ensure confidentiality and security with regard to the processing of personal data (art.17 of the DPD). For the VoIP provider, the privacy of communications is important for users and the DPD places obligations on anybody that collects personal information to take technical and organisational security measures that are appropriate to the risks presented by the processing. Subject to the exemption under art.23(2)[33] of the DPD, any breach resulting from an unlawful processing of personal data enables the user to receive some form of compensation (art.23).

Application of the Directive on Privacy and Electronic Communications 2002/58

The question that arises is what provisions apply to VoIP providers under DPEC? First, the DPEC applies to the ''processing of personal data in connection with the provision of publicly *available electronic communications services in public communications networks in the Community*'' (emphasis added). Therefore private networks are excluded within the remit of the DPEC.[34] Although there have been no legal cases in Europe on this, it could be argued that peer-to-peer VoIP service that is not provided over a *public* network but through an intranet system could fall outside the scope of the DPEC. This does not mean that the general DPD would not apply, but that the DPEC has limited its application to public communications networks.[35] The distinction drawn under the DPEC between private and public networks is unfortunate and the Article 29 Working Party (an advisory body set up under the DPD to examine data protection issues and provide opinions, make recommendations relating to data protection matters within the European Union) has not been slow to respond.

This is regrettable because private networks are gaining an increasing importance in every day life and communications of citizens, for example in the context of their work, and the risks to privacy that such networks are raising are accordingly increasing and becoming more specific (e.g. monitoring of employee behaviour by means of traffic data, lack of confidentiality of communications).

Legal obligations of VoIP providers under DPEC

For VoIP providers of publicly available networks, the following provisions that apply (not an exhaustive list) are summarised below.

Article 5 on the confidentiality of communications

Member States of the European Union are required to prohibit the '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 art.15(1) of the DPEC.

Article 6 on traffic data

Traffic data relating to subscribers and users would need to be erased or made anonymous when it is no longer needed for transmission of the communication. In the case of marketing electronic communications services or for the provision of value added services,[36] a VoIP provider could continue to process traffic data relating to subscribers/users if the subscriber/user has consented. The user/subscriber can withdraw his/her consent at any time (art.6(3) of the DPEC).

Article 4 on technical and organisational measures

The providers of a publicly available ECS would need to take appropriate technical and organisational measures to safeguard the security of their services. Examples could include measures protecting users from viruses or denial-of-services attacks.[37] Article 4(2), however, enables providers of publicly available ECS to inform subscribers of particular risks to breaches of security of the network and ''where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies''.

In the context of VoIP, one of the main questions to consider is the security of communications when users connect their ''terminals'' (be it PDAs or handheld PCs) to a public telephone network such as a WIFI hotspot. Open networks are not secure and therefore, users should generally use some form of encryption software (WEP for example) to protect the privacy of their communications between their laptop and the WIFI hotspot. However, if personal information is being uploaded or downloaded on a user's laptop, then the question is to what extent is a provider of the public electronic communications required to ensure the privacy of communications of a user's laptop when the user connects to the provider's WIFI hotspot?[38] Article 4 of the DPEC requires a provider of a publicly available ECS to take appropriate

which alone or jointly with others determines the purposes and means of the processing of personal data''.

32 European Commission, First report on the implementation of the Data Protection Directive 95/46/EC, at *http://ec.europa.eu/justice_home/fsj/privacy/lawreport/report_en.htm* [Accessed June 11, 2009], and PRIVIREAL, Data Protection—countries *http://www.privireal.org/content/dp/countries.php* [Accessed June 11, 2009].

33 DPD art.23(2) provides that ''the controller may be exempted from this liability [under the DPD], in whole or in part, if he proves that he is not responsible for the event giving rise to the damage''.

34 Article 29 Working Party, Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12 July 12, 2000, COM(2000) 385, at *http://europa.eu* [Accessed June 11, 2009].

35 DPD art.3 covers ''the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system''.

36 This is a new provision introduced under DPEC. Article 2(g) defines a ''value added service'' as ''service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof''. Examples of value added service include route guidance, traffic information, weather forecasts and tourist information that could be provided to a user or subscriber (Recital 18 of the DPEC).

37 Commission Staff Working Document, ''The treatment of Voice over Internet Protocol under the EU Regulatory Framework'', at *http://europa.eu* [Accessed June 11, 2009].

38 Compliance and Privacy, ''Wi-Fi: Are you broadcasting personal data?'', at *http://www.complianceandprivacy.com/News-Wi-Fi-broadcast-insanity.asp* [Accessed June 11, 2009].

technical and organisational measures to safeguard security of its services but this provision should also be read in the light of art.17 of the Data Protection Directive 95/46, which requires that:

> ''. . . data controllers implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing''.

Arguably, a user could also be regarded as a data controller[39] within the DPD if he or she processes personal data on his/her laptop and therefore, the privacy of communications is *not solely* the responsibility of the network or VoIP provider.

There are principally two areas of concern that need to be discussed:

> 1. *Privacy of communications*: first, defining the line between VoIP services provided over a broadband network that is operated by another internet service provider and VoIP services where the VoIP provider has control over the broadband network. The distinction is important because in the former case, it could be contended that network integrity should be maintained by the internet service provider while the VoIP provider would need to ensure the confidentiality of communications between users over this network. In the latter example, it could easily be identified that the VoIP provider has control over the network and thus, ensure the integrity of communications. Article 4(1) of DPEC, however, clearly provides that in protecting network security, the provider of a publicly available ECS may need to work with the provider of the public communications network to achieve this.[40] Therefore, preserving network integrity may have to be accomplished jointly between an internet service provider and a VoIP provider.[41]
> 2. *Spam over internet telephony*: a second area of concern that is likely to arise is the possibility of unsolicited phone calls (often referred to as spam over internet telephony or SPIT) transmitted through VoIP. Whether SPIT will become a prevalent concern as email spam is not entirely clear, but in a recent consultation[42] by OFCOM, some respondents have taken the view that anti-SPIT mechanisms are being developed to deal with this type of problem.[43] However, even though SPIT mechanisms are being developed, arguably, the current framework under the DPEC is more directed towards the traditional public telephone switch network. For example, the provision on unsolicited communications under art.13(3) requires the prior consent of subscribers in the context of automatic calling machines, fax and electronic mail. The requirement of prior consent does not necessarily apply to telephone marketing or unsolicited calls to users through VoIP; the latter is covered under art.13(3) of the DPEC. This provision enables Member States to determine the measures for unsolicited communications by means other than automated calling machines, fax and email.[44] A further point to add is that there are lists[45] which individuals can subscribe to if they do not want to be contacted by marketing companies, but presently no lists exist in the context of VoIP for individuals who do not want to be contacted using VoIP. While it should be noted that SPIT is still relatively new, it is unclear how much of a risk this will be for users.[46] Whether there should be at blacklist against potential telemarketers in VoIP is another question, but some VoIP providers such as Skype and Yahoo[47] have facilities to enable users to block certain callers. It remains to be seen whether SPIT is likely to pose a significant risk for users.

Article 9 on location data

In the case of location data,[48] processing of such data relating to users or subscribers is permitted with their consent or can only be processed when this data is made anonymous or in the case of providing a value added service,[49] could only be used with the consent of the users or subscribers. This provision is probably more relevant when considering PDAs, handheld PCs or even cell phones that uses VoIP services.

39 The definition of a ''data controller'' under art.2(d) of the DPD is broad to cover a ''natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data . . .''.

40 Article 4(1) reads as follows: ''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'' (emphasis added).

41 In an Ofcom survey, some respondents have emphasised that no VoIP service provider has control over all aspects of the network and that a VoIP provider could only reasonably be expected to deliver network integrity over the elements that it controls. For example Internet Telephony Services Providers' Association, ''Regulation of VoIP Services'', May 10, 2006, at *http://www.ofcom.org.uk/consult/condocs/voipregulation/responses/itspa.pdf* . [Accessed June 11, 2009].

42 Ofcom, ''Regulation of VoIP Services'', at *http://www.ofcom.org.uk/consult/condocs/voipregulation/voipregulation.pdf* [Accessed June 11, 2009].

43 Internet Telephony Services Providers' Association, ''Regulation of VoIP Services'', at *http://www.ofcom.org.uk/consult/condocs/voipregulation/responses/itspa.pdf* [Accessed June 11, 2009].

44 Article 13(3) reads as follows: ''Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs1 and 2 [of art.13], are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the *choice between these options to be determined by national legislation.*''

45 The UK Telephone Preference System, at *http://www.tpsonline.org.uk/tps/* [Accessed June 11, 2009].

46 Bruce Schneier, ''Combating spam'', at *http://www.schneier.com/blog/archives/2005/05/combating_spam.html* [Accessed June 11, 2009].

47 Yahoo, Regulation of VoIP services: statement and further consultation, *http://www.ofcom.org.uk/consult/condocs/voipregulation/responses/yahoo.pdf* [Accessed June 11, 2009].

48 This was a new provision introduced under the DPEC and is defined under art.2(c) as ''any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service''. For example, a computer, mobile phone or a personal digital assistant revealing the location of a user via such equipment would thus qualify as ''location data'' under art.2(c) DPEC.

49 A value added service is defined under art.2(g) of the DPEC as ''any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof''. Recital 18 of the DPEC gives examples of value added services, which may ''consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information''.

Article 15 on data retention

A controversial provision, which was subsequently approved by the European Parliament. According to the latter part of art.15(1), ''Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph [15(1)] . . .''. This provision should be read in the light of a recent Data Retentions Directive 2006/24[50] which was enacted to deal with the retention of certain data. Article 1(1) of the Data Retentions Directive expressly provides the main objective, namely to:

> ''. . . harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the *purpose of the investigation, detection and prosecution of serious crime*, as defined by each Member State in its national law''.

Data is stored between a minimum of six months to two years.[51] For internet telephony, Member States could postpone the application of the retention of communications data relating to internet telephony[52] until March 2009. The main categories of data that could be retained are data necessary to trace and identify the source of a communication[53]; data necessary to identify the destination of a communication[54]; data necessary to identify the date, time and duration of a communication[55]; data necessary to identify the type of communication; data necessary to identify users' communication equipment or what purports to be their equipment. As expressly stated under art.5(2) of the Data Retentions Directive, data revealing the content of the communications are not covered.[56] Although these provisions expressly provide the need to trace the user, the key difficulty that arises is tracing the origin of the calls that are made. In an article on VoIP,[57] Warren describes the main problems with VoIP from a law enforcement perspective:

> ''The problem with VoIP, from law enforcement perspective, is that it does not travel through an exchange. There is no simple way to catch the packets travelling over the internet, or even to link the 12-digit internet 'IP addresses' between which a call travels online to any two people. Wireless routers can generate a one time IP address that can be pinpointed to the wireless router, but—as in the case of a wireless hotspot—that will show only that the call was made from that router.''

Indeed, the problem of tracing calls is made more difficult with the use of wireless phones, wireless-enabled smart phones and PDAs that could make calls from any unlocked domestic wireless access point. In the next section, the authors consider the current legal position of the United States on the protection of VoIP.

US legal framework

The United States' use of VoIP telecommunication technologies is maturing and several of the issues discussed above have not appeared as issues in the United States. In 1928, Justice Brandeis, in *Olmstead v United States*,[58] anticipated that technological advancement would enable the Government to employ surveillance tools extending far beyond wiretapping. In that dissenting opinion, Justice Brandeis asserted that Fourth Amendment protections must be interpreted broadly to safeguard against new abuses that were not previously envisioned. Thus Brandeis sought to protect the individual's ''right to be let alone'' without regard to the different technologies that might be employed by the Government to compromise that right. Justice Brandeis's forward-looking focus on individuals' underlying privacy interests presents a more compelling perspective than the premise of the Wiretap Act as currently applied by the courts.

Since *Katz v United States*,[59] courts have routinely forbidden third parties from tapping or monitoring oral communications. However, they just as routinely permit businesses to track, store and sell data packets transmitted in the same way with the implied or explicit consent of either party engaged in the transmission. The digital age and its VoIP cause the distinction between voice and data made in the law to become muddled in the digital age. With the convergence of oral and data into a single transmission medium, the courts, like computers, are unable to distinguish between oral and data communications.[60] The use of the VoIP and analogous technologies has made this legal distinction impossible to uphold because oral and data communications now travel over the same wires simultaneously, encapsulated in digital data packets.

50 Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 [2006] OJ L105/54.

51 Article 6 of the Data Retentions Directive reads as follows: ''Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.''

52 Article 15(3) of the Data Retentions Directive provides: ''Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, *Internet telephony* and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.'' Some Member States, however, postponed the application of art.15(3) for a shorter period. For example, Austria and Germany postponed the application of the provision on the retention of communications data relating to internet access, internet telephony and internet email for 18 months after September 15, 2007.

53 Article 5(1)(a) of the DPEC. In the context of internet telephony, this the user ID; the user ID and telephone number allocated to any communication entering the public telephone network and the name and the address of the subscriber or registered user to whom an internet protocol address, user ID or telephone number was allocated at the time of the communication (art.5(1)(a)(2) of the DPEC).

54 DPEC art.5(1)(b). In the context of internet telephony, this would be the user ID or telephone number of the intended recipient(s) of an internet telephony call and the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication (art.5(1)(b)(2) of the DPEC).

55 DPEC art.5(1)(c). In the context of internet telephony, this would be the date and time of the log-in and log-off of the internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the internet access service provider to a communication, and the user ID of the subscriber or registered user; the date and time of the log-in and log-off of the internet email service or internet telephony service, based on a certain time zone (art.5(1)(c)(2) of the DPEC).

56 Recital 13 of the Data Retentions Directive provides that the Directive applies to ''data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated . . .''.

57 P. Warren, ''Lifting the veil on internet voices'', *Technology Guardian*, July 27, 2006, p.1.

58 *Olmstead v United States* 277 U.S. 438, 466, 472–74, 478 (1928) (Brandeis J. dissenting),

59 *Katz v United States* 389 U.S. 347 (1967).

60 D.B. Garrie, M.J. Armstrong and D.P. Harris, ''Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?'' (2005) 29 Seattle Univ. L. Rev. 97.

Telephone communications are protected from governmental privacy invasions

The courts have found telephone communications protected from governmental privacy invasions in two principal ways.[61] First, parties to a voice conversation are entitled to a ''reasonable expectation of privacy'' under the Supreme Court opinion of *Katz v United States*.[62] Secondly, the Federal Wiretap Act of 1968 prevents unauthorised third-party interceptions of telephone communications, unless the interceptor is in possession of a court order or either of the involved parties in the communication have provided their consent.[63] The *Katz* opinion explains the rationale behind the Supreme Court's oft-quoted statement that the Fourth Amendment ''protects people, not places'',[64] and concludes that an entity's reasonable expectation of privacy must be protected from government searches.[65] The Federal Wiretap Act was Congress's response to the *Katz* opinion and was an attempt to prevent electronic surveillance of oral telephone communications without a court order.[66]

The Supreme Court's 1967 decision in *Katz* eliminated the idea that property rights governed a person's right to be free from unreasonable searches and seizures.[67] *Katz* stands for the proposition that an individual can control which of his actions and information is accessible by the public,[68] and what remains private and protected by the Fourth Amendment.[69] The *Katz* doctrine of Fourth Amendment protections has a twofold requirement: first, a person must exhibit a subjective expectation of privacy, and secondly, that expectation must be one that society is prepared to recognise as reasonable.[70] While the courts have read *Katz* narrowly in recent years,[71] because the Fourth Amendment's privacy protections only insulate individuals from governmental privacy encroachments[72] the Wiretap Act is the main cause of action protecting telephone communicants from non-governmental third-party interceptors.[73] Telephone communicants can obtain redress under the Wiretap Act for unauthorised third-party interceptions of telephone communications unless the interceptor has a court order[74] or the consent of either party involved in the conversation.[75]

In summary, Title III of the 1968 Omnibus Crime Control and Safe Streets Act (Wiretap Act)[76] initially afforded extensive protection to wire communications, oral communications were protected only when there was a reasonable expectation of privacy.[77] Because the legislation covered both face-to-face oral communications and traditional point-to-point wired communications, courts were faced with myriad interpretive difficulties.[78] To correct the problems with Title III, Congress amended the Wiretap Act by passing the Electronic Communications Privacy Act of 1986 (ECPA).[79] Congress designed the ECPA to prohibit the intentional interception of oral, wire, and electronic communications.[80] Because Congress was concerned with advancements in electronic technology that would be capable of defeating any privacy expectations,[81] the ECPA enacted a strict set of standards for the interception of oral, wire, and electronic communications.[82] Congress further expanded the protection of wireless communication by passing the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which extended Title III to the radio portions of cellular and cordless phones.[83] In the wake of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).[84] The Patriot Act contained a number of important changes to Title III that expanded the government's ability to conduct surveillance, but it is ambiguous on what protections are extended to VoIP oral communications.

Presently, in the existing judicial environment in the United States, it is not clear whether VoIP communications will receive similar judicial treatment as oral telephone communications[85] or whether they will be treated as internet based electronic communications. The Wiretap Act's protective provisions apply equally to oral, wire, and electronic communications.[86] In practice, however, courts have permitted the interception of internet electronic communications under the Wiretap Act more than interceptions of oral telephone communications because (1) corporate web portals using clickstream technology frequently consent to the interception of end-user data for purposes of data mining, whereas telephone users rarely consent to third-party interceptions of

61 *Frierson v Goetz* 227 F. Supp. 2d 889, 896–897 (M.D. Tenn. 2002).
62 *Katz* 389 U.S. 347, 350 (1967).
63 18 USC §§2510–2521 (2004).
64 *Katz* 389 U.S. 347, 351 (1967).
65 389 U.S. 347, 353 (1967) (government's actions ''violated the privacy upon which [petitioner] justifiably relied'' and thus triggered Fourth Amendment protections).
66 *United States v Andonian* 735 F. Supp. 1469, 1471 (C.D. Cal. 1990).
67 *Katz* 389 U.S. 347, 351 (1967).
68 *Katz* 389 U.S. 347, 351 (1967) (''What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he Seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'').
69 389 U.S. 347, 352 (1967).
70 389 U.S. 347, 361 (1967) (Harlan J. concurring).
71 Orin S. Kerr, ''The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution'' (2004) 102 Mich. L. Rev. 801, 852.
72 *Skinner v Railway Labor Executives' Ass'n* 489 U.S. 602, 614 (1989); *Schmerber v California* 384 U.S. 757, 767 (1966).
73 Wiretap Act 18 USC §§2510–2521 (2004).
74 Wiretap Act 18 USC §§2511(2)(a)(ii)(A) (2004).
75 Wiretap Act 18 USC §§2511(2)(d) (2004).
76 Wiretap Act, Pub. L. No.90-351, Tit. III, §802, 82 Stat. 212 (1968).
77 *United States v McKinnon* 985 F. 2d 525, 527 (11th Cir. 1993) (stating that Congress drafted the definition of ''oral communication'' to reflect the Supreme Court's standards for determining when a reasonable expectation of privacy exists).
78 *Edwards v Bardwell* 632 F. Supp. 584, 589 (M.D. La.), aff'd, 808 F. 2d 54 (5th Cir. 1986) (treating radio telephone communications as oral communications and holding that because communications through cellular devices could easily be intercepted, the requisite reasonable expectation of privacy did not exist).
79 Electronic Communications Privacy Act of 1986, Pub. L. No.99-508, 100 Stat. 1848 (1986) (codified at 18 USC §§2510-2521, 2701–S2710, 3117, 3121–3126 (1986)).
80 S. Rep. No.99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555–3557.
81 S. Rep. No.99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555.
82 Electronic Communications Privacy Act of 1986, 18 USC §2518 (2004).
83 Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No.103-414, 108 Stat. 4279 (1994) (amending 18 USC § 2510 (2004)).
84 Patriot Act, Pub. L. No.107-56, 115 Stat. 272 (2001).
85 *Katz* 389 U.S. 347, 351–352 (1967).
86 *Bartnicki v Vopper* 532 U.S. 514, 526 (2001) (''The basic purpose of the Title III is to protect the privacy of wire *ldots* and oral communications'') (quoting S. REP. No.90-1097, at 66 (1968)).

telephone conversations[87]; (2) end-users are more likely to consent to interceptions of internet electronic communications in return for increased online functionality than they are when engaging in traditional telephone conversations[88]; and (3) internet electronic communications are more likely to be stored on an end-user's computer, making them fair game for third-party interceptors, since the Wiretap Act only applies to communications intercepted contemporaneously with transmission.[89] Therefore the US framework is currently in a state of flux and is not able to disambiguate the existing statutory language with regards to VoIP oral communication technologies.

Conclusion

As identified in the article, the regulatory framework for VoIP services both in the EU and the United States is beginning to emerge.

The European framework should be regarded as an important milestone for regulating and clarifying the provision of VoIP services; yet major questions still arise over the current classification of VoIP services, such that not all VoIP providers would be considered PATS and therefore the obligation to PATS providers would not apply to non-PATS VoIP providers such as peer-to-peer VoIP providers. Thus there is no uniformity in the legal obligations that exist for VoIP providers. As for the privacy of communications, this is principally covered under the DPD and DPEC. The main areas that need to be addressed (albeit at a European level by policymakers) is the public/private network distinction drawn under the DPEC; the preservation of network integrity between a broadband service provider and the internet service provider as covered under art.4 of the DPEC; spam over internet telephony, and tracing the origin of the caller.

While the higher expectation of privacy afforded to non-internet oral communications by the US Constitution and the Wiretap Act's prohibition of unauthorised third-party interceptions of oral telephone and electronic communications, neither the US federal courts nor legislatures have acted to explicitly protect VoIP oral internet communications[90]; in fact, as technology is evolving with respect to VoIP and oral internet communications it is becoming progressively greyer and complex in both arenas.

In order to ensure that oral communications utilising VoIP technology will receive the same treatment and protection under the law as their non-VoIP oral communication counterparts enjoy, the courts and the legislature must act. They must either explicitly recognise the legislative privacy distinction between digital data and other oral, wire and electronic communications irrespective of the issue of consent[91] or the courts must halt all use of data mining technology and wait for Congress to deliver a legislative solution. A Congressional amendment would provide courts a new legal framework in which to analyse VoIP claims brought under the Wiretap Act, enabling them to differentiate between data transmissions and other oral, data, and electronic transmissions. Without Congressional action and court application, VoIP technology remains at risk of unauthorised access and mining, which threatens the free communication of us all. The other possible solution, which is beginning to occur already, is for each state to act independently of the Federal Government; however, given the complex legal issues this approach is neither ideal nor likely to be effective in remedying VoIP communications in the United States.

87 *Chance v Avenue A, Inc* 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001).

88 A telephone communicant need not give express consent to authorise an interception under the Wiretap Act; such consent can be inferred from the surrounding circumstances. *United States v Amen* 831 F. 2d 373, 378 (2d Cir. 1987) (holding that consent can be inferred where circumstances indicate that a party knowingly agreed to surveillance), cert. denied, 485 U.S. 1021 (1988). However, inferring consent under the Wiretap Act for a telephone communication requires the party to have knowledge or notification, without which consent cannot be implied. *Re State Police Litigation* 888 F. Supp. 1235, 1266 (D. Conn. 1995) (holding that the plaintiff's claim under the Wiretap Act established sufficient evidence of an absence of either knowledge or notification to prevent the court from implying consent to the interception of a telephone communication).

AQ3

89 *Konop v Hawaiian Airlines, Inc* 302 F.• 3d 868, 878 (9th Cir. 2002) (holding that for a website to be ''intercepted'' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage). VoIP transmits in real time, offering comparable services to the traditional telephone. Philip Carden, ''Network Design Manual: Building Voice over IP, Network Computing'', at *http://www.networkcomputing.com/netdesign/1109voipfull.html* [Accessed June 11, 2009]. As with telephone communications, VoIP interceptors will usually be intercepting the communications contemporaneously with transmission. N. Borisov, I. Goldberg and D. Wagner, ''Intercepting Mobile Communications: The Insecurity of 802.11'', Seventh Annual International Conference on Mobile Computing and Networking, (July 2001); see also N. Borisov, I. Goldberg and D. Wagner, ''Security of the WEP Algorithm'', at *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.htm*. Unlike telephone communications, VoIP communications can be intercepted prior to post transmission while stored or cached on servers or end-users' computers; ''FBI Protests VoIP Approach'', January 9, 2004, at *http://www.lightreading.com/document.asp?site-lightreading&doc_id45695* [Accessed June 11, 2009]. Possibly, the courts will hold that such interceptions do not violate the Wiretap Act because the communications were not intercepted contemporaneously with transmission. In some situations, however, these VoIP interceptions may be prohibited by the Stored Communications Act, 18 USC §2701 (2004), or the Computer Fraud and Abuse Act, 18 USC §1030 (2004).

90 Garrie, Armstrong and Harris, ''Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?'' (2005) 29 Seattle Univ. L. Rev. 97.

91 Cases such as *Re DoubleClick* 154 F. Supp. 2d 497; *Re Intuit* 138 F. Supp. 2d 1272; *Re Toys R Us*, No.00-CV-2746, 2001 WL 34517252, at *1; *Chance* 165 F. Supp. 2d 1153.

THOMSON

SWEET & MAXWELL

Author: Please take time to read the below queries marked as AQ and mark your corrections and answers to these queries directly onto the proofs at the relevant place. DO NOT mark your corrections on this query sheet:

AQ1: The web pages in this and the following footnotes were obsolete and I was redirected to the main EU website.
AQ2: I was unable to open the web page in the footnote—can you check the address or give the date you last accessed it, please?
AQ3: I was unable to access the web page for ''Security of the WEP Algorithm'' in the footnote—can you check the address or give the date you last accessed it, please?