REGULATING VOICE OVER INTERNET PROTOCOL: AN E.U./U.S. COMPARATIVE APPROACH

DANIEL B. GARRIE & REBECCA WONG*

* Daniel B. Garrie is the CEO of LegalTech Group LLC, a firm specializing in providing large compliance with complex technology compliant solutions. Mr. Garrie is a lawyer in New York and New Jersey. He has penned several law review articles on a variety of technology and legal issues. Mr. Garrie has worked around the world with the various government agencies and corporations as a Senior Consultant. Mr. Garrie currently resides in New York City. Mr. Garrie can be reached at Daniel@legaltechgroup.com.

Rebecca Wong is Lecturer in Law, Nottingham Law School, Nottingham Trent University. Her main areas of specialty are in data protection and privacy. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and has recently completed her PhD in data protection.

I. 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.[1] In this paper, we consider the extent to which VoIP services are protected from an E.U./U.S. perspective and the concerns arising from the current legislative framework, mainly from a privacy perspective. This paper is divided into three parts. Part II considers VoIP services in general. Part III examines the European framework and in particular, the current categorization of VoIP services before considering the privacy perspective, taking into account the Directive on Privacy and Electronic Communications 2002/58/EC ("DPEC")[2] and the general Data Protection Directive 95/46/EC ("DPD").[3] Part IV considers the U.S. framework in protecting the privacy of communications, asserting that the federal courts and legislatures should act to explicitly protect VoIP oral Internet communications. Part V will conclude by discussing the principal areas that still need to be addressed.

1. *See* David Bach & Jonathan Sallet, *The Challenges of Classification: Emerging VOIP Regulation in Europe and the United States*, FIRST MONDAY, June 14, 2005, http://www.firstmonday.org/issues/issue10_7/bach/ (supplying a starting point into the classification of VoIP services). Bach and Sallet address the need for regulation and different methods that could be used, as well as providing an analysis of the issues surrounding the different methods of regulation available.

2. *See* Council Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC) [hereinafter DPEC] (addressing the European Parliament and the Council of the European Union's concerns with protecting the privacy of personal data across borders).

3. *See* Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC) [hereinafter DPD] (addressing the processing, protection, and free movement of personal data).

II. WHAT IS VOICE OVER INTERNET PROTOCOL?

In its broadest definition, VoIP can be described as the "conveyance of voice, fax and related services partially or wholly over packet-switched IP-based networks, including peer-to-peer VoIP services and VoIP services connected to PSTN."[4] According to the latest estimate, more than 18.7 million people worldwide were using retail VoIP services by the end of 2005.[5] This figure is increased to nearly twenty-four million when PC-based VoIP services such as Skype are included.[6] While these figures indicate a rising trend in the take-up of VoIP services by users, the question arises on the main issues that dominate VoIP services and its regulation within Europe and the United States. For the purposes of this paper, we shall consider the narrow interpretation of VoIP to refer to voice traffic carried over Internet Protocal ("IP") based broadband Internet networks.

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 IP networks, and vice versa.[7] VoIP transforms standard oral telephone signals into

4. Organization for Economic Co-operation and Development [OECD], Directorate For Science, Technology and Industry Committee For Information, Computer And Communications Policy, Working Party on Telecommunications and Information Services Policies, *Policy Considerations of VOIP*, 4 (March 21, 2006), *available at* http://www.oecd.org/dataoecd/59/55/36316212.pdf.

5. Point Topic, *Retail VoIP Subscribers Increase by 83% During 2005*, August 16, 2006, http://www.point-topic.com/content/dslanalysis/BBAVoipana060816.htm.

6. *Id.*

7. *See* Peter Grant, *Ready for Prime Time: A New Internet-Based Phone Technology has an Un-Catchy Acronym: VoIP*, WALL ST. J., Jan. 12, 2004, at R7 (describing the emergence of VoIP and providing an overview of the emerging market for VoIP services). Growth projections for VoIP vary widely, but the Wall Street Journal reported that "[b]y the end of this year [2004], about 20% of the new phones being shipped to U.S. businesses will use VOIP technology, according to Yankee Group, a technology consulting firm based in Boston. By 2007 that figure should exceed 50%, and eventually almost all of the new phones shipped will use VoIP, Yankee Group predicts." *Id.*

compressed data packets that are sent over the Internet using Internet Protocol.[8] The audio signal at this point is captured in an analog format either by way of a microphone or received from a line input device,[9] and converted to a digital representation at the audio input device.[10] The resulting digital samples are copied into a memory buffer in blocks of frame length.[11] Here, a silence detector decides whether the block is silence or a portion of speech, and removes the silent blocks to speed transmission of the digital data.[12] 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.[13] Once this step is complete, the block of samples is copied from the buffer to the audio output device.[14] The audio output device makes the digital to analog conversion and outputs the signal.[15] VoIP can be used with either a telephone or a PC as the user terminal.[16] This allows different modes of operation: PC to PC, PC to telephone, telephone to PC and telephone to telephone

8. *See generally* UYLESS BLACK, VOICE OVER IP 1 (1995) (introducing the basic terms and concepts of Internet Protocol and VoIP).

9. *See* Jon-Olov Vant, *IP Telephony: Mobility and Security* 15 (May 2005) (doctoral thesis in teleinformatics, Stockholm, Sweden) (describing the means of capturing audio data at its source and the process by which it is transferred onto a packet based network); *see, e.g.*, TELECOMM. STANDARDIZATION SECTOR OF ITU [ITU-T], INT'L TELECOMM. UNION, ITU-T RECOMMENDATION H.225.0, CALL SIGNALLING PROTOCOLS AND MEDIA STREAM PACKETIZATION FOR PACKET BASED MULTIMEDIA COMMUNICATION SYSTEMS 67–69 (1998) (providing a technical description of how multicast services such as interactive audio and video are delivered via a packet based network).

10. Vant, *supra* note 9, at 16.

11. *Id.* at 16–17.

12. *Id.* at 17.

13. *See generally*, Philip Carden, *Building Voice over IP*, NETWORK COMPUTING, May 8, 2000 (describing the different technologies a home or business could use in an effort to switch over from traditional phone systems to a VoIP phone system).

14. *See generally* Darrin Woods, *Connecting to the Voice World*, NETWORK COMPUTING, April 17, 2000 (explaining the various ways to switch from standard PBX telephony to newer VoIP telephony).

15. Vant, *supra* note 9, at 20.

16. *See* Rachael King, *Home of the Future*, TELEPHONY, June 6, 2005, at 10 (predicting that consumers will begin replacing their cordless telephones with telephone handsets capable of handling VoIP services).

(via the Internet). All VoIP protocols are application layer protocols.[17]

For some time, people have been aware of the potential for wiretapping, but the public perceives such actions to be limited to corporate espionage and criminal activities.[18] Eavesdropping over the switched telephone network requires physical access to the telephone line and access to some type of hardware device that may or may not be very sophisticated.[19] Wiretapping dangers increase considerably in the VoIP world. The equipment or software needed is much more sophisticated, but well within the reach of a sixteen-year old hacker that has access to e-Bay or the Web. Data sniffing tools[20] are readily

17. *See* BLACK, *supra* note 8, at 23–24 (explaining that the application layer is the seventh layer of the Open Systems Interconnection (OSI) Model and provides services for end-user applications such as file transfers, e-mail, and other network software services). The application layer is defined within the OSI Model and utilizes TCP/IP protocols, which are an industry standard group of protocols through which computers find, communicate, and access one another over a transmission medium. *Id.* at 41–51. The protocol group is implemented in the form of a software package known as a TCP/IP stack, which splits the transmission into a number of discrete tasks. *Id.* Each layer corresponds to a different form of communication, and the TCP/IP architecture utilizes four layers; application, transport, Internet, and the physical layer. *Id.* The transmission of voice communications over the Internet initiates with data being sent from the application layer down the stack to physical layer, where it is then transmitted to the receiver and ascends the stack in reverse order, ending at the application layer. *Id.* at 23–24.

18. *See* Jay Fitzgerald, *Team to Tie Net Phone Hackers; Industry Aims to Stop Scams Before They Start*, BOSTON HERALD, April 26, 2005, at 31 (reporting that businesses are starting up a national organization to develop security measures which will prevent VoIP eavesdropping before "hackers inevitably turn their attention to the growing VoIP").

19. *See* K. Percy & M. Hommer, *Tips From the Trenches on VoIP*, NETWORK WORLD, Jan. 27, 2003, at 48 (recognizing that eavesdropping on standard PBX phone lines requires physical access to the phone system's hardware or phone lines themselves). Percy and Hommer describe eavesdropping on a VoIP network as "the most dreaded form of deviant behavior," recommending that VoIP users take the proper precautions to prevent the behavior. *Id.* VoIP vendors and equipment providers are taking the appropriate steps to prevent this behavior by adding security features to their offerings. *Id.*

20. *See* P.J. Bruening & M. Stephen, *Spyware: Technologies, Issues, and Policy Proposals*, 7 J. INTERNET L. 3, 3–5 (2004) (explaining how data sniffing tools, such as cookie technology, spyware, and adware, pose a threat to computer security). Data sniffing tools are used primarily to steal or transmit end-user data from an end-users machines with or without their knowledge. *Id.* Advertisers can use these tools to identify what sites end-users have visited and deliver targeted ads

available and these tools will soon be enhanced to become aware of the new VoIP protocols, broadening access to wiretapping tools.[21] While in an office environment VoIP traffic travels over a data network that is used by all of the regular users of the corporate LAN (local area network), any or all of the conversations traversing a network could theoretically be compromised by anyone with a regular connection on the network.[22] Consequently, VoIP packets could be identified and stored for re-assembly to be played back at a later time.[23] The idea that only Internet traffic is at risk is simply wrong.[24] Privacy for oral traffic could be vastly enhanced by the use of encryption.[25] Most corporate and home networks, however, do not encrypt VoIP calls.[26]

---

to the end-user's computer. *Id.* For example, if a user visits a Florida cruise site followed by a later visit to a golfing site, advertisers using data sniffing tools will serve advertisements to the end-user's computer about golf course vacations in Florida.

21. *See Scumware.biz Educates About Dangers of Adware/Scumware*, 5 COMPUTER SECURITY UPDATE 2 (Feb. 2004) (describing one such tool, Scumware, that allows publishers to monitor individuals' browsing activity).

22. *See* Dale J. Long, *The Lazy Person's Guide to Voice Telephony—Part II*, CHIPS MAGAZINE, Spring 2004, at 43–44 (recognizing that attempts to intercept communications are likely to grow with the widespread adoption of wireless network technologies).

23. *See* Amie J. Singer, *Cost-Effectiveness, Security Concerns at Heart of Uncertainty: Debate Over Voice-Over Internet Protocol Benefits*, SAN DIEGO BUS. J., Dec. 17, 2001.

24. *See* Ian 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 WKLY, Apr. 19, 2005, at 34.

25. *See* Philip Bednarz, Communications Design Conference, *Security Considerations at Forefront of VoIP Design*, ELECTRONIC ENGINEERING TIMES, Sept. 23, 2002, at 63 (noting that "data encryption is the best defense against eavesdropping"). The author, however, acknowledges that encryption and decryption can delay packets, causing problems with two-way conversations if the overall latency of a VoIP call is greater than approximately 250 milliseconds. *Id.*

26. *See* Yumi Nishiyama, Collective Action in a Complex Environment: The Case Study of Network Security in Telecom/IT Convergence 3, 15–16 (Apr. 24, 2003) (unpublished Master's thesis, Georgetown University) (on file with author) (explaining that VoIP is a solid technology; however, it requires government regulation to ensure a certain level of product reliability and safety for the consumer). Up until today, the users have seen security issues in the data and voice worlds as completely separate. 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. *Id.* at 1,

One of the attractive features provided by VoIP is the ability to locate intelligence at various points in the network. Gatekeeper or call-manager type devices, which authenticate users and establish connections,[27] can physically reside on any server[28] on the network. This is really a two-edged sword. Logging information about user calls may be useful for billing or tracking purposes, but these logs can also become targets for hackers. If this type of information becomes compromised, it can create serious concerns for organizations or individuals.[29] Unfortunately, the home user and the majority of corporate users are unaware of any of these vulnerabilities when they purchase or use VoIP technology.[30]

8. VoIP is vulnerable because convergent technologies lead to weakness from multiple points. *Id.* at 11, 34. In addition, VoIP must address the security holes in cell phones that arise from the transport mechanisms used when mobile phones are used. *See* Martius Miettinen, *IT-Security in the Automobile Domain*, 6 (2003), *available at* http://www.cs.helsinki.fi/u/mjmietti/seminaariS03/automobilesecurity.pdf.

Adjoining these problems is the reality that cell tracker tools have evolved and people can eavesdrop with much greater ease on cellular transmission. *Id.* Also, hackers can intercept data with greater ease than before when the data travels in soft zones (unprotected) between legitimate users and cell towers. *Id.* Thus, transmitting information in digital form raises new vulnerabilities and digital devices can be used for fiscal and/or privacy violations. *Id.* at 17, 23. As the VoIP systems run on vulnerable software, they must contend with all of these possible holes.

27. *See* Michele Rosen, *The Maturing of the Internet Telephony Market—Market is Maturing—Internet/Web/Online Service Information*, ENT, Mar. 18, 1998, at 48 (stating that a gatekeeper is an optional component of an H.323 enabled network that provides central management and control services). H.323 is a technical standard that defines protocols which enable VoIP companies to create interoperable Internet telephony solutions. *Id.* Gatekeepers usually deliver the following in relation to VoIP services: (1) address translation; (2) bandwidth management; and (3) routing functionality. *Id.*

28. *See* Oxford English Dictionary Online, Server (last visited Apr. 8, 2007) ("In a network, any program which manages shared access to a centralized resource or service; an (often dedicated) device on which such a program is run.").

29. *See* Edwin Mier et al., *VoIP Security Wares; Breaking Through IP Telephony,* NETWORK WORLD, May 24, 2004, at 84–88.

30. *See* Fitzgerald, *supra* note 18 (reporting that many firms are developing security measures to protect the growing sector of VoIP services against the next wave of computer hackers). *See generally* Mike Lee, *Beware! Bugs Can Attack Net Phones; They May be Cheap But They Are Also Vulnerable to Hackers, Say Experts, Who Advise Installing Anti-Virus Patches*, STRAITS TIMES (Singapore), Aug. 22, 2004 (explaining that VoIP phones are extremely vulnerable to hackers because hackers need no specialized equipment to tap into Internet phones).

III. EUROPEAN FRAMEWORK FOR THE PROTECTION OF VOIP SERVICES

A. 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[31] which was principally concerned with reforming the telecommunications sector. The NRF is comprised of five Directives: the Framework Directive 2002/21/EC,[32] Authorisation Directive 2002/20/EC,[33] Access and Interconnection Directive 2002/19/EC,[34] Universal Service Directive 2002/22/EC,[35] and the Directive on Privacy and Electronic Communications 2002/58/EC.[36]

The Framework Directive sets out the main principles and objectives underpinning the E.U. regulatory policy on the provision of electronic communications services and networks, including the role of the National Regulator Authority ("NRA").[37] The Access and Interconnection Directive deals with the harmonization of the linking of networks between operators of public communications services.[38]

31. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions Towards a New Framework for Electronic Communications Infrastructure and Associated Services: The 1999 Communications Review*, COM (1999) 539 (Nov. 10, 1999).

32. Council Directive 2002/21, On a Common Regulatory Framework for Electronic Communications Networks and Services, 2002 O.J. (L 108) 33 (EC) [hereinafter Framework Directive 2002/21].

33. Council Directive 2002/20, On the Authorisation of Electronic Communications Networks and Services, 2002 O.J. (L 108) 21 (EC).

34. Council Directive 2002/19, On Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, 2002 O.J. (L 108) 7 (EC) [hereinafter Access Directive 2002/19].

35. Council Directive 2002/22, On Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, 2002 O.J. (L 108) 51 (EC) [hereinafter Universal Service Directive 2002/22].

36. DPEC, *supra* note 2.

37. Framework Directive 2002/21, *supra* note 32.

38. Access Directive 2002/19, *supra* note 34.

The Universal Services Directive is important because it principally deals with the minimum set of services to be made available to end-users including Publicly Available Telecommunications Services ("PATS"),[39] network integrity, directory enquiry services, public payphones and special measures for disabled users.[40] The Authorisation Directive establishes a legal framework for Member States on general authorization[41] and applies to the authorization of all public and private electronic communications networks[42] and electronic communications services.[43] By covering "all electronic communications networks and services" whether provided publicly or not, the Directive applies to both categories of providers so that they can "benefit from objective, transparent, non-discriminatory and proportionate rights, conditions and procedures." [44]

39. *See infra* notes 56–67 and accompanying text.

40. *See* European Commission, *Universal Service*, http://europa.eu.int/information_society/policy/ecomm/todays_framework/universal_service/index_en.htm (last visited Aug. 10, 2006) (explaining that "universal service" is "a safety net to ensure that a set of basic telecommunications services would always be available at a determined quality and affordable price, even if the market would not provide it").

41. *See* European Commission, *Regulating Market Access*, http://europa.eu.int/information_society/policy/ecomm/todays_framework/market_access/index_en.htm (last visited Aug. 10, 2006).

42. Framework Directive 2002/21, *supra* note 32, art. 2(a) (defining an "'electronic communications network'" as "transmission systems and, where applicable, switching or 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, fixed (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 type of information conveyed . . .").

43. *Id.* art. (2)(c) (defining an "'electronic communications service'" as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks . . .").

44. Access Directive 2002/19, *supra* note 34, Recital 4.

In 2004, the Analysys Report[45] commissioned by the European Commission, was published which considered the subject of VoIP services. Amongst the issues discussed, the report examined the regulation, structure of the telecoms market and current technology used.[46] In particular, the report authors took the view that the following issues needed to be addressed. Namely, the current categorization of VoIP as PATS, location independence, emergency access, and network integrity.[47] Given the scope of this paper, the discussion will focus on the current categorization of VoIP from a U.S. and European perspective.

B. CLASSIFICATION OF VOIP PROVIDERS

In brief, the regulation of VoIP in Europe is slightly complex[48] because there is no consensus over the categorization of VoIP 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 PATS. An ECS is defined under Art. 2(c) of the Framework Directive as a "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks."[49] Therefore, a VoIP service that provided a product such as a software program to be run on a personal computer with no ongoing provision of service would fall outside the scope of the E.U. regulatory framework.[50] A PATS is

45. *See* European Commission, *Final Report for the European Commission: IP Voice and Associated Convergent Voices*, (Jan. 28, 2004) (prepared by Analysys), *available at* http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/studies_ext_consult/ip_voice/401_28_ip_voice_and_associated_convergent_services.pdf.

46. *Id.* at i–iii.

47. *Id.* at iii.

48. *See* Bach & Sallet, *supra* note 1; Ian Walden, *European Union Communications Law*, *in* TELECOMMUNICATIONS LAW AND REGULATION 107 (Ian Walden & John Angel eds., 2d ed. 2005); Sirge J.H. Gijrath. *Voiding the Regulation or Regulating the Void? Voice Over Internet Protocol and Voice Over Broadband in the Netherlands*, 12 COMPUTER & TELECOMM. L. REV. 150, 150–155 (2006); Katrina Dick, *The Emergence and Regulation of VoIP*, 10 COMPUTER & TELECOMM. L. REV. 157, 157–59 (2004).

49. Framework Directive 2002/21, *supra* note 32, art. 2(c).

50. *See* European Commission, *Commission Staff Working Document on the Treatment of Voice Over Internet Protocol Under the EU Regulatory Framework* §

defined under Art. 2(c) of the Universal Directive 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."[51]

The classification of a VoIP provider as PATS means that the criteria laid down under the Universal Services Directive would apply.[52] 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 categorization of VoIP providers as PATS is not wholly conclusive. In response to a consultation paper on the *treatment of voice over internet protocol*[53] by the European Commission, the European Internet Service Providers Association ("EuroISPA") made known their view the need for legal certainty regarding the rights and obligation of the VoIP service providers.[54] In particular, they added that "VoIP providers should not be classed as a PATS provider on the basis of certain technical parameters."[55] They took the view that "VoIP provider[s] should be categorized as a PATS provider if its service is assessed from the demand side (i.e. the customer) as a direct substitute for their traditional voice telephony service."[56] Arguably, the demand for VoIP services has not reached the point where it has replaced the traditional telephony service,[57] but the lack

3 (June 14, 2004) (prepared by Information Society Directorate-General), *available at* http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf.

51. Universal Service Directive 2002/22, *supra* note 35, art. 2(c).

52. *Id.*

53. European Commission, *supra* note 50.

54. *See* European Internet Services Providers Association [EuroISPA], *DG INFSO Information and Consultation Document: The Treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework: Response from EuroISPA* 2 (2004), *available at* http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/voip/eispa.pdf (arguing that robust implementation of the regulatory framework will encourage innovation and new entrants into the market).

55. *Id.* at 2.

56. *Id.*

57. *See* Olli Mattila, Background for Discussions at ERG Meeting 17.46.04, *Voice over IP (VoIP) – Background and Regulatory Aspects*, *available at* http://erg.eu.int/doc/publications/consult_accounting_sep/erg_0422_voip_discussi

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,[58] 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.[59] The TeliaSonera's VoIP Service was offered only to their broadband users and was offered as a substitute for pubic switched telephone network ("PSTN") connection. The implication arising from the Ficora's decision was that the TeliaSonera VoIP Service had to comply with the obligations set for PATS laid down under the Finnish regulations. These included making available to their users, access to the international calls using the access code 00, availability to 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 itemized bills free of charge to the user.[60]

The United Kingdom's NRF, Ofcom has used the same criterion as the Universal Services Directive by holding the view that a provider qualifies as a PATS if *all* the following criteria are 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."[61] What this means is that a VoIP provider based in

on_note.ppt (last visited Aug. 8, 2006) (predicting that the expansion of broadband internet access is likely to accelerate the use of VoIP services). 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 and less than 20,000 VoIP users in Europe. *Id.*

58. Finnish Communications Regulatory Authority, *Decision of the Finnish Communications Regulatory Authority on Compliance with Law of the Sonera Puhekaista Service* (Oct. 29, 2003), http://www.ficora.fi/englanti/document/SoneraPuhekaista.pdf.

59. *Id.* at 10.

60. *Id.* at 11–12.

61. Ofcom, Office of Communications, *Regulation of VoIP Services* 95 (2006),

the United Kingdom, which does not meet all the criteria described above would *not* be considered as PATS.[62]

Whilst the criterion to qualify as PATS is clear, it is unclear what the obligations are for VoIP providers that do not qualify for PATS status. Certainly, such non-PATS providers, such as peer-to-peer VoIP providers, would not have to fulfill the obligations as required under the Universal Services Directive; however, some VoIP providers may constitute an ECS as defined under the Framework Directive or corresponding national legislation and therefore will be required to comply with the obligations laid down under the NRF.[63] More specifically, a provider would have to adhere to the Authorisation Directive because it applies to ECS and the DPEC.[64] The latter protects the privacy of communications in the electronic communications sector. The DPEC replaces the Telecommunications Directive 97/66/EC[65] by dealing with the processing of personal data in the context of the electronic communications sector. It complements the general DPD,[66] 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 organization or individual that collected personal information, be required to adhere with the general DPD[67] or corresponding national legislation. The DPD was passed to harmonize the data protection laws within the European Union[68] and

available at http://www.ofcom.org.uk/consult/condocs/voipregulation/voipregulation.pdf.

62. *Id.*

63. Framework Directive 2002/21, *supra* note 32, art. 2(c) (defining electronic communications service as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks").

64. DPEC, *supra* note 2.

65. Council Directive 97/66, Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1997 O.J. (L 24) 1 (EC).

66. DPD, *supra* note 3.

67. DPEC, *supra* note 2.

68. For a background history into data protection laws in Europe, see LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS (2002); COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2003); and Andrew

imposes certain obligations on organizations or individuals ("data controllers")[69] that process personal information to comply *inter alia* with the data protection principles as laid down under Art. 6 of the DPD or its corresponding national laws.

Art. 6 requires that personal data must be:

> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[70]

Charlesworth, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures*, 54 HASTINGS L.J. 931 (2003).

69. DPD, *supra* note 3, art. 2(d) (defining "data controllers" as "the 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 ").

70. *Id.* art. 6.

All the Member States of the European Union have corresponding provisions to Art. 6 of the DPD.[71] Individuals whose personal information is collected by the data controllers are entitled to 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.[72] Furthermore, data controllers are required to "implement appropriate technical and organizational measures" to ensure confidentiality and security with regard to the processing of personal data.[73] 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 organizational security measures that are appropriate to the risks presented by the processing. Subject to the exemption under Art. 23(2) of the DPD,[74] any breach resulting from an unlawful processing of personal data enables the user to receive some form of compensation .[75] As alluded to earlier, the DPD is supplemented by the DPEC.[76]

C. APPLICATION OF THE DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS

The question that arises is what provisions under DPEC, if any, apply to VoIP providers? 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*."[77] Therefore, *private networks* are excluded within the remit of the DPEC.[78] Although

71. *See* European Commission, *First Report on the Implementation of the Data Protection Directive 95/46/EC*, COM (2003) 265 final (May 15, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/lawreport/report_en.htm. *See generally*, Privacy in Research Ethics & Law [PRIVIREAL], Data Protection – Countries, *available at http://www.privireal.org/content/dp/countries.php*.

72. DPD, *supra* note 3, art. 10.

73. *Id.* art. 17(1).

74. *See id.* art. 23(2) ("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.").

75. *See id.* art. 23(1).

76. *See* DPEC, *supra* note 2.

77. *Id.* art. 3(1) (emphasis added).

78. *See* Working Party on the Protection of Individuals with Regard to the

there have been no legal cases in Europe on this, it could be argued that peer-to-peer VoIP service that are not provided over a *public* network but through an intranet system could fall outside the scope of the DPEC. Although the DPEC would not apply under the example given, the general DPD would continue to apply.[79] The distinction, however, drawn under the DPEC between private and public networks is unfortunate and the Art. 29 Working Party[80]—an advisory body set up under the DPD to *inter alia* examine data protection issues, and provide opinions and 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).[81]

For VoIP providers that do provide a service over a *publicly available electronic communications service,* the following provisions under DPEC would apply:

Processing of Personal Data [Data Protection 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 of 12 July 2000 COM (2000) 385*, (Nov. 2, 2000) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf.

79. *See id.* at 3; *see also* DPD, *supra* note 3, art. 3 (setting forth the broad scope of the DPD which 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").

80. *See* DPD, *supra* note 3, arts. 29, 30 (detailing the role of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data). The roles include examining questions about national measures adopted under the DPD, giving opinions on level of protection in member countries and third-party countries, and making "recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community").

81. Data Protection Working Party, *supra* note 78, at 3.

1. 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 Article 15(1) [of the DPEC]."[82] Art. 15(1) of the DPEC enables Member States to "adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5,[83] Article 6,[84] Article 8(1),[85] (2), (3), (4), and Article 9[86] of this Directive when such restriction constitutes a *necessary, appropriate and proportionate measure within a democratic society to safeguard national security* (i.e. State security), *defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system,* as referred to in Article 13(1) of [the Data Protection] Directive 95/46/EC."[87]

2. 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.[88] In the case of marketing electronic communications services or for the provision of value added services,[89] a VoIP provider could continue to process traffic

82. DPEC, *supra* note 2, art. 5(1).

83. *See id.* (providing for the confidentiality of communications).

84. *See id.* art. 6(1) (stating that public communications network providers must erase traffic data relating to subscribers and users or make the information anonymous when no longer needed by the provider to transmit the communication). Article 2(b) defines "traffic data" as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof ." *Id.* art. 2(b).

85. *See id.* art. 8 (covering the presentation and restriction of calling and connected line identification of users).

86. *See id.* art. 9 (providing that location data may only be processed anonymously or with the consent of the users). This is a new provision introduced under the DPEC.

87. *Id.* art. 15(1) (emphasis added).

88. *See id.* art. 6(1).

89. *See id.* art. 2(g) (defining "value added service" as a "service which requires the processing of traffic data or location data other than traffic data

data relating to subscribers/users if the subscriber/user has consented. The user/subscriber can withdraw his/her consent at any time.[90]

3. Article 4 on Technical and Organizational Measures

The providers of a publicly available ECS would need to take "appropriate technical and organisational measures to safeguard the security of its services."[91] Examples could include measures protecting users from viruses or denial-of-services attacks.[92] Art. 4(2) however, enables providers of publicly available ECS to inform subscribers of particular risks to breaches of security of the network "where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies."[93]

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?[94]

Art. 4 of the DPEC requires a provider of a publicly available ECS to take "appropriate technical and organisational measures to

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. *Id.* Recital 18.

90. *See id.* art. 6(3).

91. *Id.* art. 4(1).

92. *See* European Commission, *supra* note 50, § 5.5.1.

93. DPEC, *supra* note 2, art. 4(2).

94. *See* Compliance and Privacy. *Wi-Fi: Are You Broadcasting Personal Data?* http://www.complianceandprivacy.com/News-Wi-Fi-broadcast-insanity.asp (last visited Apr. 8, 2007) (noting that anyone nearby with access to the same network could access a user's PC unless some basic security is in place, such as, a firewall, password-controlled access, or end data encryption).

safeguard security of its services,"[95] but this provision should also be read in the light of Art. 17 of the DPD, 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."[96]

It should also be added that a user could also be regarded as a data controller[97] 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 needs to be discussed. 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 whilst 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, can ensure the integrity of communications. Art. 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.[98] Therefore, preserving network integrity may have to be accomplished jointly between an Internet service provider and a VoIP provider.[99]

95. DPEC, *supra* note 2, art. 4(1).

96. DPD, *supra* note 3, art. 17(1).

97. *See id.* art. 2(d).

98. *See* DPEC, *supra* note 2, art. 4(1) (establishing that "[t]he 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).

99. *Cf.* In an Ofcom survey, some respondents have emphasised that no VoIP

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 ("SPIT"))[100] transmitted through VoIP. Whether SPIT will become a prevalent concern, like e-mail spam, is not entirely clear, but in a recent consultation by the U.K. NRA, Ofcom some respondents have taken the view that anti-SPAM/SPIT mechanisms are being developed to deal with this type of problem.[101]

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 e-mail.[102]

---

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. *See*, e.g., Internet Telephony Services Providers' Association [ITSPA], *Regulation of VoIP Services* 2, 23 (2006), http://www.ofcom.org.uk/consult/condocs/voipregulation/responses/itspa.pdf.

100. *See* Ofcom, *supra* note 61, at 75.

101. *See* ITSPA, s*upra* note 99, at 21; *see also* Celeste Biever, *Move over Spam, Make Way for "Spit"*, NEW SCIENTIST, Sept. 24, 2004, *available at* http://www.newscientist.com/article.ns?id=dn6445; Posting of Bruce Schneier to Schneier on Security, *Combating Spam*, http://www.schneier.com/blog/archives/2005/05/combating_spam.html (May 13, 2005); Ben Charny, *Net Phone Customers Brace for 'VoIP Spam'*, CNET NEWS, Aug. 23, 2004, http://news.com.com/Net+phone+customers+brace+for+VoIP+spam/2100-7352_3-5302988.html; Eyeball Networks, Eyeball AntiSPIT™ Server, http://www.eyeball.com/products/anti_spit_server.html (last visited Mar. 15, 2007).

102. *See* DPEC, *supra* note 2, art. 13(3) ("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 paragraphs 1 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*.") (emphasis added).

A further point to add is that there are lists (telephone preference systems)[103] whereby individuals can subscribe 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. Whilst it should be noted that SPIT is still relatively new, it is unclear how much of a risk this will be for users.[104] Whether there should be a blacklist against potential telemarketers in VoIP is another question, but some VoIP providers such as Skype and Yahoo[105] 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.

4. Article 9 on Location Data

In the case of location data,[106] 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,[107] could only be used with the consent of the users or subscribers.[108] This provision is probably

103. *See*, *e.g.*, Telephone Preference Service, Welcome to TPS Online, http://www.tpsonline.org.uk/tps/ (last visited Aug. 26, 2006) (describing the "Telephone Preference Service" (TPS) which allows end-users to limit access of their telephone number and prevent access by certain organizations and other solicitors).

104. *See* Schneier, *supra* note 101.

105. *See* Yahoo! UK & Ireland, *Regulation of VoIP Services: Statement and Further Consultation* 6 (2006), http://www.ofcom.org.uk/consult/condocs/voipregulation/responses/yahoo.pdf, at Ques. 25 (providing a Yahoo! Messenger with BT Communicator service which enables customers to block communication from senders on their "ignore" list).

106. *See* DPEC, *supra* note 2, art. 2(c) (defining the term "location data" 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) of the DPEC. *See also* Linda Ackerman, James Kempf & Toshio Miki, *Wireless Location Privacy: Law and Policy in the US, EU and Japan* (2003), *available at* http://www.isoc.org/briefings/015/index.shtml.

107. *See* DPEC, *supra* note 2, art. 2(g).

108. *See id.* art. 9 (stating for location data other than traffic data "[t]he service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to

more relevant when considering PDAs, handheld PCs or even cell phones that uses VoIP services.

5. Article 13 on Unsolicited Communications

As discussed earlier, this provision was introduced to deal with the problem of spam.[109] Prior/opt-in consent of subscribers is required when unsolicited communications are sent using automated calling systems, e-mails and faxes.[110] However, in the case of existing customers, a natural and legal person may send unsolicited communications by e-mail on an opt-out basis.[111]

6. 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)]."[112] This provision should be read in the light of a recent Data Retentions Directive 2006/24/EC,[113] which was enacted to deal with the retention of certain data. Art. 1(1)

---

a third party for the purpose of providing the value added service").

109. *See* Lilian Edwards, *Articles 6–7; Privacy and Electronic Communications Directive 2002: Canning the Spam and Cutting the Cookies: Consumer Privacy Online and EU Regulation*, *in* THE NEW LEGAL FRAMEWORK FOR E-COMMERCE IN EUROPE 46 (2005).

110. *See* DPEC, *supra* note 2, art. 13(1) ("The use of automated calling systems without human intervention (automated calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their *prior* consent.") (emphasis added).

111. *See id.* art. 13(2) ("[W]here a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.").

112. *Id.* art. 15(1).

113. *See* Council 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/EC, 2006 O.J. (L 105) 54 (EC).

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. [114]

Data is stored between a minimum of six months to two years.[115] For internet telephony, Member States can postpone the application of the retention of communications data relating to Internet telephony until March 2009.[116] The main categories of data that could be retained are data necessary to trace and identify the source of a communication,[117] data necessary to identify the destination of a communication,[118] data necessary to identify the date, time and

114. *Id.* art. 1(1) (emphasis added).

115. *See id.* art. 6 ("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.").

116. *See id.* art. 15(3) ("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*.") (first emphasis added). Some Member States, however, have postponed the application of Art. 15(3) for a shorter period. For example, Austria and Germany have postponed the application of the provision on the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for 18 months after 15 September 2007. *Id.* Declaration by Austria and Germany.

117. *See id.*, art. 5(1)(a). In the context of internet telephony, Member States shall ensure "the user ID and telephone number allocated to any communication entering the public telephone network" and "the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication" are retained. *Id.* art. 5(1)(a)(2).

118. *See id.* art. 5(1)(b) (asserting that in the context of internet telephony, Member States shall ensure the retention of "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

duration of a communication,[119] data necessary to identify the type of communication,[120] and data necessary to identify users' communication equipment or what purports to be their equipment.[121] As expressly stated under Art. 5(2) of the Data Retentions Directive,[122] data revealing the content of the communications are not covered.[123]

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 a recent article on VoIP,[124] 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.[125]

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. The Data Retentions Directive goes some way to make it mandatory for VoIP providers to retain data relating to users, but

recipient of the communication").

119. *See id.* art. 5(1)(c) (indicating that in the context of internet telephony, Member States will ensure the retention of "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" and "the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone").

120. *See id.* art. 5(1)(d).

121. *See id.* art. 5(1)(e)(3).

122. *Id.* art. 5(2).

123. *See id.* Recital 13 (providing 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").

124. Peter Warren, *Lifting the Veil on Internet Voices,* GUARDIAN (London), July 27, 2006, at Technology 1.

125. *Id.*

whether users can be sufficiently identified or with any degree of certainty is not entirely clear.

D. CONCLUSION CONCERNING THE EUROPEAN FRAMEWORK

To summarize, the European framework[126] should be regarded as an important milestone for regulating and clarifying (though not exclusively) 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) are 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.

126. At the time of writing, the European Commission is currently reviewing the electronic communications framework with amendments anticipated to take place starting in 2009. In the context of privacy, the main changes include an explicit obligation under Art. 4(1) of the DPEC between electronic communications networks providers and electronic communications service providers to co-operate in ensuring data security. The discussion of the changes are beyond the scope of this article, but a good starting point would be the European Commission Information Society Website, *Roadmap for the Reform of the EU's Telecom Rules*, http://europa.eu.int/information_society/policy/ecomm/tomorrow/roadmap/index_en.htm#implementation_report, (last visited Mar. 15, 2007); Hogan & Hartson LLP & Analysys, Final Report for the European Commission, *Preparing the Next Steps in Regulation of Electronic Communications: A Contribution to the Review of the Electronic Communications Regulatory Framework* (July 2006), *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/studies_ext_consult/next_steps/regul_of_ecomm_july2006_final.pdf.

IV. U.S. FRAMEWORK[127]

In 1928, Justice Brandeis, in *Olmstead v. United States*,[128] anticipated that technological advancement would enable the Government to employ surveillance tools extending far beyond wiretapping.[129] 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' 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.[130]

Since *Katz v. United States*,[131] courts have routinely forbidden third parties from tapping or monitoring oral communications. However, they just as routinely permit business 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 causes the distinction between voice and data made in the law to become muddled in the digital age.[132]

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. The use of the VoIP and Similar technologies has made this legal distinction impossible to

127. The U.S. use of VoIP telecommunication technologies is maturing and several of the issues discussed above in the European section have not been heard by the U.S. courts.

128. 277 U.S. 438, 472–74, 478 (1928) (Brandeis, J., dissenting).

129. *Id. See generally* Daniel B. Garrie, Matthew J. Armstrong & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U. L. REV. 97 (2005) (examining Voice Over Internet Protocol communications and whether Title III of the Omnibus Crime Control and Safe Street Act of 1968 [Wiretap Act] applies to this new type of communication).

130. Garrie, Armstrong & Harris, *supra* note 129, at 100.

131. 389 U.S. 347 (1967) (holding that the wiretapping of a public telephone booth violated the Fourth Amendment and constituted a search and seizure).

132. Garrie, Armstrong & Harris, *supra* note 129, at 100.

uphold because oral and electronic data communications now travel over the same wires simultaneously, encapsulated in digital data packets.[133]

A. TELEPHONE COMMUNICATIONS ARE PROTECTED FROM GOVERNMENTAL PRIVACY INVASIONS

The courts have found telephone communications protected from governmental privacy invasions in two principal ways.[134] First, parties to a voice conversation are entitled to a "reasonable expectation of privacy" under the Supreme Court opinion of *Katz v. United States*.[135] Second, the Federal Wiretap Act of 1968 prevents unauthorized 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.[136] The *Katz* opinion explains the rationale behind the Supreme Court's oft-quoted statement that the Fourth Amendment "protects people, not places,"[137] and concludes that an entity's reasonable expectation of privacy must be protected from government searches.[138] The Federal Wiretap Act was Congress'

133. *Id.* at 100–01.

134. *See* Frierson v. Goetz, 227 F. Supp. 2d 889, 896–97 (M.D. Tenn. 2002) (describing a two-part test for determining qualified immunity). "First, courts must decide whether the alleged constitutional or statutory violations were 'clearly established' at the time of the alleged violations." *Id.* at 896. Second, the court decides "'whether a reasonable person in the defendant's position would have known that his or her actions violated clearly established rights.'" *Id.* at 896–97 (quoting Blake v. Wright, 179 F.3d 1003, 1008 (6th Cir. 1999)).

135. *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring) (explaining that when in a phone booth, "a person has a constitutionally protected reasonable expectation of privacy" and that "electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment"). The *Katz* Court suggests that a man who enters a phone booth and closes the door behind him reasonably expects that his conversation will not be overheard. *Id.* at 352.

136. 18 U.S.C. §§ 2510–2521 (2004).

137. *See Katz,* 389 U.S. at 351 (explaining that the Fourth Amendment does not protect what a person wittingly or deliberately exposes to the public but does protect anything a person "seeks to preserve as private, even in an area accessible to the public").

138. *See id.* at 353 (holding that the government's actions "violated the privacy upon which [petitioner] justifiably relied," and thus triggered Fourth Amendment protections). However, it is unclear how the recent action by the Bush administration respective to wiretapping will be interpreted by the Supreme Court

response to the Katz opinion and was an attempt to prevent electronic surveillance of oral telephone communications without a court order.[139]

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.[140] Katz stands for the proposition that an individual can control which of his actions and information is accessible by the public,[141] and what remains private and protected by the Fourth Amendment.[142] The Katz doctrine of Fourth Amendment protections has a twofold requirement: first, a person must exhibit a subjective expectation of privacy, and second, that expectation must be one that society is prepared to recognize as reasonable.[143] While the courts have read Katz narrowly in recent years,[144] and the Fourth Amendment's privacy protections only insulate individuals from governmental privacy encroachments,[145]

---

under the context of National Security interplaying with the constitutionally granted rights of the executive privilege.

139. *See* United States v. Andonian, 735 F. Supp. 1469, 1471 (C.D. Cal. 1990); S. REP. NO. 90-1097, at 38, 46–47 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153, 2162–63.

140. *See* 389 U.S. at 353 (discrediting the notion that a court must find a "trespass," and clarifying that no physical intrusion need occur to implicate Fourth Amendment protections).

141. *See id.* at 351 (holding that "[w]hat 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").

142. *See id.* at 351–52 (alluding to the fact that while the public could see petitioner using the telephone, Petitioner's actions in closing the door to the booth indicated his intent to prevent the public from hearing his conversation).

143. *See id.* at 361 (Harlan, J., concurring).

144. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case For Caution*, 102 MICH. L. REV. 801, 852 (2004) (stating that "despite Berger and Katz, courts have proved surprisingly reluctant to find that the occasional holes in the Wiretap Act violate the Fourth Amendment"). Moreover, "wiretapping law may be constitutional in theory, but it is statutory in practice . . . [w]hen wiretapping occurs inside the United States, courts generally refuse to construe the Fourth Amendment as going beyond the scope of the Wiretap Act." *Id.* at 855.

145. *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 613 (1989) (stating that "[a]lthough the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government"); *see also* Schmerber v. California, 384

the Wiretap Act is the main cause of action protecting telephone communicants from non-governmental third-party interceptors.[146] Telephone communicants can obtain redress under the Wiretap Act for unauthorized third party interceptions of telephone communications unless the interceptor has a court order[147] or the consent of either party involved in the conversation.[148]

> While Title III of the 1968 Omnibus Crime Control and Safe Streets Act (hereinafter "Wiretap Act") initially afforded extensive protection to wire communications, oral communications were protected only when there was a reasonable expectation of privacy. Because the legislation covered both face-to-face oral communications and traditional point-to-point wired communications, courts were faced with myriad interpretive difficulties. To correct the problems with Title III, Congress amended the Wiretap Act by passing the Electronic Communications Privacy Act of 1986 (ECPA). Congress designed the ECPA to prohibit the intentional interception of oral, wire, and electronic communications. Because Congress was concerned with advancements in electronic technology that would be capable of defeating any privacy expectations, the ECPA enacted a strict set of standards for the interception of oral, wire, and electronic communications. 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. 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). The Patriot Act contained a number of important changes to Title III that expanded the government's ability to conduct surveillance.

U.S. 757, 767 (1966) (stating that "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State").

146. *See* 18 U.S.C. §§ 2510–2521.

147. *See id.* § 2511(2)(a)(ii) (noting that a written certification from an individual authorized under the statute also will suffice, but both the order and certification must specify the duration, information to be gathered, and facilities to be used).

148. *See id.* § 2511(2)(d).

. . . .

> In the existing judicial environment, it is not clear whether VoIP communications will receive similar judicial treatment as oral telephone communications 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. 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 telephone conversations; (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; 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.[149]

Therefore, the U.S. 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.

The issue gets even more complicated with the expansive reach of globalization. For instance, what if a user in the United States uses a VoIP line that goes thru Europe while being routed to a peer within the United States and a third party intercepts the transmission in Canada and is not a U.S. citizen?[150] The U.S. courts do not have a

149. Garrie, Armstrong & Harris, *supra* note 129, at 114, 120–21 (footnotes omitted).

150. The network over which the call is transmitted can be a few feet or thousands of miles. *See* Washington Exch. Carrier Ass'n v. LocalDial Corp., Final Order Granting Motions for Summary Determination, Dkt. No. UT-031472 at 11 (Wash. Utils. & Transp. Comm'n June 11, 2004) ("For a call from Seattle to Spokane or from Olympia to Bellingham, this whole process of converting the call from TDM to IP and back to TDM again occurs in the room at the Westin Building.")

clear answer[151] and there is no clear state or federal regulatory response.[152] Thus, the average U.S. consumer using a VoIP phone for their conversations has little recourse against a foreign third-party interceptor of their conversation. The consumer might be able to assert a cause-of-action against the U.S. VoIP provider, depending of course on the circumstances, but it is not clear whether such a suit would be successful.

V. CONCLUSION

As identified in the paper, the regulatory framework for VoIP services both in the European Union and the United States is beginning to emerge. In the European Union, VoIP services are principally covered under the new regulatory framework for electronic communications. In the context of privacy of communications, this is dealt with under the DPD [153] and the DPEC.[154] In the United States, VoIP services are not covered by explicit regulatory bodies to VoIP communications; however, and unlike in Europe, the scope of privacy still remains ambiguous and unresolved in the United States. The main areas of concern that need to be addressed at a global level (Europe and the United States) include the issue of spam over Internet telephony, network integrity shared between a VoIP provider and the Internet service provider,

151. *See*, *e.g.,* Ben Charny, *Minnesota: Phone Rules Apply to VoIP*, CNET NEWS, Aug. 21, 2003, *available at* http://zdnet.com.com/2100-1104_2-5066652.html; Ashley H. Grant, *Judge: Internet Phone Regulation Could Slow Net's Expansion*, USA TODAY.COM, Oct. 17, 2003, http://www.usatoday.com/tech/news/techpolicy/2003-10-17-netphone-ruling-logic_x.htm; W. David Gardner, *Minnesota Judge: VoIP is Unregulated Data*, TECHWEB, Oct. 8, 2003, http://www.techweb.com/wire/story/TWB20031008S0017.

152. *See In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, 28 F.C.C. 2d 267, ¶¶ 27, 31–38 (Mar. 18, 1971) (final decision and order); *see also In re* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, 28 F.C.C. 2d 291, ¶¶ 39–45 (Apr. 3, 1970) (tentative decision); *In the Matter of* a Study of Voice over Internet Protocol, Case No. TW-2004-0324, Order Establishing Case (Mo. Pub. Serv. Comm'n Feb. 3, 2004), http://www.psc.mo.gov/teleco/VOIP_Order.pdf.

153. *See* DPD, *supra* note 3.

154. *See* DPEC, *supra* note 2.

and caller identification under VoIP (such as tracing the origin of the caller).

While the higher expectation of privacy afforded to non-Internet oral communications by the U.S. Constitution[155] and the Wiretap Act's prohibition of unauthorized third-party interceptions of oral telephone and electronic communications,[156] neither the U.S. federal courts nor legislatures have acted to explicitly protect VoIP oral Internet communications;[157] 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 utilizing VoIP technology will enjoy the same treatment and protection under the law as their non-VoIP oral communication counterparts, the courts and the legislature must act. They must either explicitly recognize the legislative privacy distinction between digital data and other oral, wire and electronic communications irrespective of the issue of consent[158] or the courts must halt all use of data mining technology

155. *Compare* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronically listening to telephone conversations constitutes a "search and seizure within the meaning of the Fourth Amendment") *with* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (concluding that "[c]yberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis").

156. *See* United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976) (holding that a violation of the Act required that interception occur contemporaneously with transmission); *see also* 18 U.S.C. § 2511(1) ("any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication . . . shall be punished . . . or shall be subject to suit . . ."); Maryland v. Garrison, 480 U.S. 79, 90 (1987) (Blackmun, J., dissenting); Segura v. United States, 468 U.S. 796, 810 (1984) ("The sanctity of the home is not to be disputed."); *Katz*, 389 U.S. at 353 (declaring that use of electronic eavesdropping equipment to overhear conversation inside telephone booth intrudes on legitimate expectation of privacy); City of Indianapolis v. Edmond, 531 U.S. 32, 54 (2000) (Rehnquist, C.J., dissenting) (describing body and home as areas "ordinarily afforded the most stringent Fourth Amendment protection").

157. *See* Garrie, Armstrong & Harris, *supra* note 129.

158. *See In re DoubleClick, Inc.*, 154 F. Supp. 2d 497, 510 (S.D.N.Y. 2001); *In re* Intuit, 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001); *In re* Toys R Us, No. 00-CV-2746, 2001 WL 34517252, at *3–4 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1160–62 (W.D. Wash. 2001). In each case, the court held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's

and wait for Congress to deliver a legislative solution.[159] A Congressional amendment would provide courts a new legal framework in which to analyze 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 unauthorized 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 the situation of VoIP communications in the United States.

communications with the Web site, it was done with the consent of the Web site, which was a party to the communication. *But see In re* Pharmatrak, Inc., 329 F.3d 9, 20–21 (1st Cir. 2003) (finding that there was no consent under the Wiretap Act, 18 U.S.C. § 2511(2)(d) (2004), where a corporate entity had an explicit agreement prohibiting a third-party from collecting personal identifiable information).

159. *See Pharmatrak*, 329 F.3d at 21–22.