NETWORK NEUTRALITY:

LAISSEZ-FAIRE APPROACH OR NOT?

REBECCA WONG[*] & DANIEL B. GARRIE[†]

[*] Rebecca Wong is Senior Lecturer in Law at Nottingham Law School, Nottingham Trent University, with teaching and research interests in tort, intellectual property, data protection, privacy and cyber law. She holds an LLB (1998), MSc (2000), LLM (2001), PCHE (2004) and has recently completed her PhD (University of Sheffield, 2007) in data protection. Her recent publications have included *Data Protection Online: Alternative approaches to sensitive data*, 2 INT'L J. COM. L. & Tech 9 (2007) (reprinted in Journal of Internet Law, March 2007 and ICFAI Cyberlaw, May 2007) and *Demystifying clickstream data: a European and US perspective* 20EMORY INT'L REV. 2, 563 (2006).

†. Mr. Daniel Garrie, Esq. is a Principal in the Legal-Business Consulting practice at CRA International – formerly Charles Rivers Associates. Mr. Garrie specializes in legal technology risk management. He consults primarily to in-house counsel and IT departments on information management strategies in the United States and internationally, e-policy guidance synchronization (policies and operations), e-discovery litigation risk management and legal technology strategies, integration, and best practices. Prior to joining CRA, Mr. Garrie was a vice president of LegalTech Group where he provided subject matter expertise and project management in engagements pertaining to e-Discovery, vendor selection, litigation readiness, digital privacy, and digital information risk management. Mr. Garrie is admitted to practice law in New York and New Jersey, and currently serves as editor-in-chief of the Journal of Legal Technology Risk Management. He has a M.A. and a B.A in Computer Science from Brandeis University and a J.D. from Rutgers School of Law. Mr. Garrie has published more than 30 articles in scholarly and industry legal journals worldwide, and his writings are widely cited in legal and technology publications. Please feel free to e-mail Mr. Garrie at daniel.garrie@gmail.com.

The authors were panelist members on the Network Neutrality panel in the IASTED Law and Technology Conference, Berkeley, California held in September 2007. A shortened version of the paper was presented at the Legal Security and Privacy Issues Conference, Beijing 2007. Grateful acknowledgments to the participants for their feedback.

The authors would like to thank the contributions of Jeff Hodge in writing this article and Tom Kiedrowski, Russell Richardson, and Ofcom for their initial feedback. Views given in this article are entirely those of the authors.

ABSTRACT

The paper discusses the subject of network neutrality from an American and European legal perspective. While acknowledging the plethora of literature on network neutrality, it argues that regulation in favor of network neutrality should not be confined within the U.S./European borders, but rather network neutrality should be addressed from a global perspective through the OECD/WTO. The article will begin by defining network neutrality before discussing the technology underpinning network neutrality. It will compare the different legal approaches adopted by Europe and the United States to the regulation of network neutrality. In Europe, there is an existing electronic communications regulatory framework, which can be used to address the network neutrality problem. In particular, this article will examine the Access and Interconnection Directive, arguing that further regulations at the European level are not necessary given the legal infrastructure. The main concerns arising from the United States' unilateral stance is whether it will cause a digital divide in the electronic communications market. Legislation in the area of network neutrality is not perceived as necessary in Europe. Any regulation at a European level would disrupt the existing electronic communications framework. In the United States, network neutrality appears to be the only viable legal path. Network technology violates the spirit of the U.S. Wiretap Law and several State specific privacy laws. The article will conclude that the United States' stance to adopt network neutrality legislation will cause a seismic shift in the way we view technology.

> . . . Analysis shows that calls for network neutrality regulation are justified: In the absence of network neutrality regulation, there is a real threat that network providers will discriminate against independent producers of applications, content or portals or exclude them from their network. This threat reduces the amount of innovation in the markets for applications, content and portals at significant costs to society.
>
> Van Schewick, 2005.[1]

> There is no indication that network operators have any plans to gather and store personally identifiable information at the router level but policy makers should be aware that the widespread adoption of packet shaping technologies at least gives operators the ability to flag packets based on the payload (contents) of the packet and the IP address of the user. This could, in turn, raise fears that data could be easily processed for purposes unrelated to traffic routing. The privacy issues may be complex under a multi-tiered Internet structure and could warrant particular attention by privacy specialists.
>
> OECD, Internet Traffic Prioritisation: an overview 2007.[2]

I. INTRODUCTION

While network neutrality has been the subject of heated debate in the United States, the topic has received far less attention on a global scale. In this paper, the authors explore network neutrality from a European and U.S. standpoint with particular focus on the international implications arising from the unilateral stance adopted by the United States in legislating on network neutrality. The arguments in favor of network neutrality regulation should not be confined to the United States, as they apply to other nations as well.

1. Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 40 (2005), http://www.lessig.org/blog/archives/b_paper.pdf.

2. OECD, Working Party on Telecommunication and Information Services Policies, Internet Traffic Prioritisation: An Overview, 27 (Apr. 4, 2007), http://www.oecd.org/dataoecd/43/63/38405781.pdf.

In this paper, the authors address some of the arguments advanced in favor of network neutrality including consumer protection and the need to prevent companies and countries from blocking their network services to consumers. Is it simply a power struggle between the applications and content providers fighting to use the same network and determine who governs? Some of these questions have already been debated by legal scholars such as Wu and Yoo.[3] We will, however, explore the imbalance that may be created by network neutrality legislation introduced in the U.S. in preventing essential services such as emergency responses, 911 calls, and VoIP connections from being efficiently delivered because of the potential costs that may apply.

This paper is divided into four sections. The first section will examine the notion of network neutrality as defined by Wu and Berners Lee and define the scope of "network neutrality" as it relates to this paper.

The second and third sections will discuss the current European and U.S. legal framework. The differences in the network infrastructure are examined in light of the contrasting legal framework in the United States and Europe, specifically, the lack of a sufficient legal framework in the United States as opposed to the European Framework and in particular, the Access and Interconnection Directive. Although not expressly provided, implicit within the Access and Interconnection Directive is the network neutrality principle, a conclusion that is discussed by the provisions dealing with significant market power (SMP) and non-SMP operators.

II. "NETWORK NEUTRALITY"

The term "network neutrality" can be regarded as a misnomer when applied to the Internet, since the Internet, or at least its use (in monetary terms), is not free. Several definitions exist of network neutrality. Perhaps the most well known is given by Professor Wu:[4]

3. Christopher S. Yoo & Tim Wu, *Keeping the Internet Neutral?: Christopher S. Yoo and Timothy Wu Debate,* Columbia University Law School: Center for Law & Economics Studies Research Paper, No. 310, *available at* http://ssrn.com/abstract=953989, (last visited Apr. 2, 2008).

4. TimWu.org, Network Neutrality FAQ, http://www.timwu.org/network_

> Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized – when they are a platform for multiple uses, present and future.[5]

Sir Tim Berners Lee, creator of the world wide web, however, defines network neutrality as follows: "If I pay to connect to the net with a given quality of service, and you pay to connect to the net with the same or higher quality of service, then we can communicate at that level."[6]

In this paper, the term "network neutrality" applies to the provision of Internet applications/services by Internet service providers, in the context of *wireless*[7] and *wired* communications.[8] *Companies* and even *countries* should not block access to the use of services/software applications that end users (consumers) would like to be offered. It is preferable to use the term *"non-prioritization or non-discrimination of communications"* between Internet service providers and content/application providers on the Internet.

According to Yoo, the U.S. proposals on network neutrality come down to this:

> Network neutrality proposals are aimed at preserving competition in applications and content, which are those portions of the industry that are already the most competitive and the least protected by entry barriers . . . . Instead, the real focus should be on the impact network neutrality regulation would have on the competitiveness of the last-mile.[9]

---

neutrality.html (last visited Mar. 25, 2008).

5. *Id.*

6. Sir Tim Berners Lee, *Net Neutrality: This is Serious,* http://dig.csail.mit.edu/breadcrumbs/node/144 (last visited Jan 27, 2007).

7. Examples of mobile devices include mobile phones and PDAs.

8. This distinction is important because there has been a recent paper published by Wu noting that wireless networks are not playing by the same rules as wired networks. *See* Eric M. Zeman, *Paper Sparks Wireless Net Neutrality Debate,* http://freepress.net/news/21377, (last visited Mar. 10, 2007).

9. Yoo & Wu, *supra* note 3, at 6 (emphasis added).

Is it simply a matter of preventing discrimination between ISP providers and content providers accessing the Internet (wireless or not)? If so, what are the implications for the privacy of users' browsing activities and, more specifically, the privacy of communications[10] on the Internet be it within Europe or the United States? This is explored later.

A further point is that if network neutrality regulation is embraced, enforcement will be a difficult issue. How effective will enforcement be? This will be a matter for the national regulatory authorities and in particular, those that monitor access to each Internet service provider. While legislative measures can be beneficial, it can have the effect of being cumbersome upon enforcement authorities such as the FCC and telecommunication authorities (OFCOM in the United Kingdom, etc.) which do not have the sufficient resources to monitor how networks can block access.[11]

How do regulators deal with Internet Service Providers who operate outside of, and block applications from the United States? Irrespective of whether this is a European problem, networks are not confined within a finite border.[12]

The existing literature has focused on the main arguments that have been asserted in favor of *network neutrality regulation* in the United States. This can be summarized as follows:

10. Directive 2002/58/EC on Privacy and Electronic Communications protects the privacy of *public* electronic communications networks, but does not include private networks. The latter is protected under the general European Data Protection Directive 95/46, 1995 O.J. (L281) 31 (EC). For a discussion of the application of the Data Protection Framework to clickstream data, *see also* Daniel B. Garrie & Rebecca Wong, *Demystifying Clickstream Data*, 20 EMORY INT'L L. REV. 563 (2006).

11. *See* Christopher T. Marsden. *Net neutrality and consumer access to content*, 4:4 *SCRIPT-ed* 407 (2007), at http://www.law.ed.ac.uk/ahrc/script-ed/vol14-4/marsden.asp; and Michael Geist. *ISPs New Role in Network Control*, BBC NEWS, Jan. 29, 2008, *available at* http://news.bbc.co.uk/2/hi/technology/7215235.stm.

12. On the subject of Internet borders, *see* Joel R. Reidenberg. *Governing Networks and Rule-making in Cyberspace*, 45 EMORY L. J. 911 (1996); David R Johnson and David G. Post. *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); and Michael A. Froomkin. *The Internet as a Source of Regulatory Arbitrage*, http://osaka.law.miami.edu/~froomkin/articles/arbitr.htm, (last visited Mar. 13, 2007).

CONSUMER CHOICE: The underlying rationale submitted by authors such as Wu and Lessig are that companies who block the service are depriving or degrading the quality of services that can be passed on to the consumer. Wu argues that "blocking can keep a better or cheaper product (VoIP) from coming to market at all, and often it can prevent such products from being offered in an effective form."[13] To give an example, Skype had recently applied to the Federal Communications Commission to rule that consumers should be entitled to attach whatever mobile devices they can on their mobile phone networks (Carterfone rules).[14] Although this was not shared by the cell phone industry, CTIA, it illustrates that consumers could effectively be prevented from installing VoIP clients by phone providers (whether this could be circumvented technically is another question).

There is also the PUBLIC AND PRIVATE PROPERTY ARGUMENT: the broadband connections are public resources and should be used to convey data irrespective of where it originates. In other words, "a bit is a bit, whether it is part of someone's e-mail, an Internet voice over Internet conversation or as part of a pirated movie."[15] Arguably, consumers are entitled to resources on the Internet without interference from broadband providers.

PRIVACY OF COMMUNICATIONS[16]: This subject, which seems to be neglected as network neutrality regulation, has often been associated with the prevention of anti-competitive behavior by ISPs/broadband providers that block access of their networks to content providers. Thus, network neutrality regulation aims to

13. Tim Wu & Christopher S. Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575, 578 (2007).

14. Marguerite Reardon, *Skype Petitions FCC for Open Cellular Access*, CNET, Feb. 22, 2007, http://news.com.com/2100-1036_3-6161569.html?part=rss&tag=2547 -1_3-0-20&subj=news; Eric M. Zeman, *Paper Sparks Wireless Net Neutrality Debate*, FREEPRESS, Feb. 28, 2007, at http://freepress.net/news/ 21377; The Technology Liberation Front, *Skype Asks FCC to Impose Carterfone; Regs on Wireless*, TECH. LIBERATION FRONT, Feb. 22, 2007, http://www.techliberation. com/archives/042060.php.

15. Victoria Shannon, *The End User: Neutrality? Yes and No,* INT'L HERALD TRIB., Sept. 12, 2006, at 18, *available at* http://www.iht.com/articles/2006/06/21/business/ptend22.php.

16. *See* Molly Wood, *Net Neutrality: Bring it on,* CNET, June 30, 2006, http://www.cnet.com/4520-6033_1-6548559-1.html.

present a level playing field for content and application providers with modem and Digital Service Line (or Broadband) providers. However, the privacy of communications is an important issue for users, particularly if users want to decide whether the packets on the Internet are blocked by their Internet service provider. Additionally, networks referred to here are *packet switched networks* (rather than circuit switched networks that apply to telecommunications), which divide the data into packets. This is commonly used in VoIP calls.[17] In Europe, there are two main Directives that cover the protection of personal information.[18] There is the general Data Protection Directive that covers the protection of personal information in the online and offline environment[19] and the Directive on Privacy of Electronic Communications (DPEC), a specific Directive aimed at the "electronic communications sector."[20] The DPEC complements and particularizes the DPD and applies to "public communications" (private networks are excluded). The E.U. Member States have transposed both Directives into their own legislation.[21] The privacy of communications is not absolute[22] however, because the

17. *See* Daniel B. Garrie & Rebecca Wong, *Regulating Voice Over Internet Protocol: An E.U./U.S. Comparative Approach*, 22 AM. U. INT'L L. REV. 549, 551-55 (2007) (detailing the origin and definition of VoIP technology). VoIP is the use of Internet Protocol data connections for communications that have traditionally been carried over the public switched telephone network. Voice over Internet Protocol (VoIP) FCC Consumer Facts, http://www.fcc.gov/cgb/consumerfacts/voip.pdf (last visited Mar. 27, 2008) [hereinafter VoIP Consumer Facts].

18. Art. 1(1) of the Data Protection Directive 95/46/EC expressly provides for the protection of fundamental rights and freedoms including privacy. Official Journal of the European Communities of 23 November 1995 No L. 281, Council Directive 95/46, art. 1(1), *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_27 [hereinafter DPD].

19. By offline, Art. 3(1) of the DPD limits protection of files that "form part of a filing system or intended to form part of a filing system." *Id.* art. 3(1).

20. Directive on Privacy of Electronic Communications, Official Journal of the European Communities of 12 July 2002 No L. 201, Council Directive 2002/58 art. 15(1), *available at* http://www.dataprotection.ie/documents/legal/directive2002_58.pdf [hereinafter DPEC].

21. *See* European Commission, *Analysis and Impact Study on the Implementation of Directive 95/46/EC in Member States, available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf (last visited Mar. 12, 2007).

22. Art. 15(1) of the Directive on Privacy of Electronic Communications

exemptions, including national security, provided under Art. 13 of the DPD,[23] may still apply. Companies may find themselves subject to the DPD and DPEC as "data controllers"[24] because they process personal information of individuals. In the context of electronic communications, a relevant example would be an Internet service provider that holds information of its users. For example, Internet service providers such as AOL and BT[25] would hold information of its subscribers. It is possible for Internet service providers to block access of content providers such as Skype to some but not all of its users based on their IP addresses. In some ways, this would be a form of discrimination. Whether discrimination is overtly done is less than clear. However, the OECD has recently published a report entitled *Internet Traffic Prioritization*,[26] which aimed to examine policy and regulatory issues surrounding traffic prioritization. The report acknowledged that anti-competitive behaviour in the broadband market will be an important determinant when deciding whether regulation is

2002/58/EC provides that

> Member States may adopt legislative measures to restrict the scope of the rights and obligations for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restrictions 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 communications system, as referred to in Article 13(1) of [Data Protection] Directive 95/46/EC . . . .

DPEC, *supra* note 20, art. 13(1).

23. Art. 13 of the DPD enables EU Member States to adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security (b) defence (c) public security (d) the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Council Directive 95/46, *supra* note 18, art. 13.

24. "Data controllers" are defined broadly under the DPD 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 . . . ." *Id.* art. 2(d).

25. Hypothetical example given.

26. OECD, *Internet Traffic Prioritisation: An Overview*, DSTI/ICCP/TISP(2006)4/ FINAL, *available at* http://www.oecd.org/dataoecd/43/63/38405781.pdf (last visited Apr. 23, 2008).

necessary to guard against traffic prioritization.[27] In the context of monitoring the types of packets that travel in the routers, the report makes the following observations:

> Packet shaping technologies give network operators the ability to examine header information and the payload of packets before making decisions on how the packets are then delivered. Network operators have long had the ability to examine data in the packets flowing over their networks but the proposition of a multi-tiered Internet significantly increases the number of routers that would actively be examining packets . . . . There is no indication that network operators have any plans to gather and store personally identifiable information at the router level but policy makers *should be aware that the wide spread adoption of packet shaping technologies at least gives operators the ability to flag packets based on the payload (contents) of the packet and the IP address of the user.* This could, in turn, raise fears that data could be easily processed for purposes unrelated to traffic routing. The privacy issues may be complex under a multi-tiered Internet structure and could warrant particular attention by privacy specialists.[28]

Any monitoring of web pages accessed by individuals should be limited to what is necessary and in accordance with the European Data Protection Directive[29] and Directive on Privacy and Electronic Communications.[30] More transparency is needed on the part of network operators if the privacy of users' web browsing activities is to be maintained. This is beyond the scope of this study, but is intended to highlight some of the issues that exist with Internet filtering.

27. *See id.*

28. *Id*. at 27 (emphasis added).

29. *See* Council Directive 1995/46, 1995 O.J. (L281) 31 (EC), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited Apr. 27, 2008).

30. *See* Council Directive 2002/58, 2002 O.J. (L201) 37-47 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF (last visited Apr. 27, 2008).

III . EUROPEAN LEGAL FRAMEWORK

A. New Regulatory Framework for Electronic Communications

While the debate on network neutrality regulation in the United States has been extensive, this topic has received considerably less attention in Europe. The focus by the European Commission this year has been on improving the existing regulatory framework on electronic communications through national regulatory authorities (NRAs).[31] The regulatory framework is comprised of five main Directives. These are the Framework Directive[32]; the Authorisation Directive[33]; the Access Directive[34]; the Universal Service Directive[35]; and the Directive on privacy and electronic communications.[36] In this section, the authors will not go into detail over the Directives as this has been covered elsewhere,[37] but consider the Access Directive given its centrality to the discussion on network neutrality. The Access Directive enables undertakings to negotiate interconnection with other network providers of public electronic communications networks.[38] It does not apply to private

31. *See* Council Directive 2002/21, 2002 O.J. (L 108) 33 (EC), art. 3, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF (last visited Apr. 29, 2008) [hereinafter Framework Directive]. For in-depth reading into the framework, *see* TELECOMMUNICATIONS LAW AND REGULATION (Ian Walden & John Angel eds. 2d ed. 2005); Europe's Information Society, *Telecoms in the European Union*, http://ec.europa.eu/information_society/ policy/ecomm/index_en.htm (last visited Apr. 29, 2008).

32. Framework Directive, *supra* note 31.

33. Council Directive 2002/20, 2002 O.J. (L 108) 21 (EC), *available at* eur-lex.europa.eu/pri/en/oj/dat/2002/l_108/l_10820020424en00210032.pdf (last visited Apr. 27, 2008) [hereinafter Authorisation Directive].

34. Council Directive 2002/19, 2002 O.J. (L108) 7 (EC), *available at* http://www.anacom.pt/streaming/2002.19.EC.pdf?categoryId=59430&contentId=94585&field=ATTACHED_FILE (last visited May 5, 2008) [hereinafter Access Directive].

35. Council Directive 2002/22, 2002 O.J. (L 108) 51 (EC), *available at* http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_108/l_10820020424en00510077.pdf (last visited May 5, 2008) [hereinafter Universal Service Directive].

36. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:047:EN:PDF [hereinafter Directive on Privacy and Electronic Communication].

37. *See generally* Garrie & Wong, *supra* note 10.

38. Access Directive, *supra* note 34, arts. 1.1, 1.2.

networks. Instead, the aim of the Directive is to harmonize the "way in which Member States regulate access to, and interconnection of, electronic communications networks and associated facilities."[39] The approach by the Directorate of Information Society is to take a liberal view to telecommunications such that it is left to the "undertaking" to negotiate interconnection agreements.

First, we should consider the main definitions provided under the Access Directive.[40] The Access Directive applies to networks "carrying publicly available communications services" including "fixed and mobile telecommunications networks."[41] It does not apply to web-based content,[42] but to Internet access providers. This is an important point to make because the distinction drawn under the Framework Directive could therefore mean that ISPs providing web-based content fall outside the realm of the Access Directive[43], and thus, the Access Directive has its own limitations. In the absence of a possible remedy (by requiring operators to open access to their networks), it is possible, to use existing competition law or national legislation implementing competition law to enable access to networks.[44] However, it does appear unfortunate that potential competitors providing web-based contents should be

39. *Id.* art. 1.1. For a background into the EU telecommunications framework, *see* Ian Walden, *European Union Communications Law, in* TELECOMMUNICATIONS LAW AND REGULATION 107, 107-149 (Ian Walden & John Angel, eds., 2003); TELECOMMUNICATIONS LAW IN EUROPE (Joachim Scherer ed., 5ed. 2005) (1993); Europe's Information Society, *Tomorrow's Framework: Roadmap for the 2006 Review*, *available at* http://ec.europa.eu/information_society/policy/ecomm/tomorrow/roadmap/index_en.htm (last visited Apr. 30, 2008). *See also* Consolidating the Internal Market for Electronic Communications, COM(07)(401) final, *available at* www.parliament.gov.mt/information/Papers/7992(C).doc (last visited Apr. 30, 2008).

40. *See* Access Directive, *supra* note 34.

41. Europa – Gateway of the European Union, Access to Electronic Communications Networks, para. 3, *available at* http://europa.eu/scadplus/leg/en/lvb/l24108i.htm (last visited April 4, 2008).

42. *But see* Framework Directive, *supra* note 31, art. 2(c) (electronic communications services does not include "services providing, or exercising editorial control over, content transmitted using electronic communications networks and services . . . .").

43. *See* TELECOMMUNICATIONS LAW IN EUROPE, *supra* note 39, at 69.

44. *Id.*

excluded from the Access Directive.

Returning to the definitions under the Access Directive, "operator" is defined as an "undertaking providing or authorised to provide a public communications network or an associated facility."[45]

An "electronic communications network" is defined as "a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description" together with any "apparatus comprised in the system" and "software and stored data."[46]

"Access" means the "making available of facilities and/or services to another undertaking . . . for the purpose of providing electronic communications services."[47]

The main provision that is noteworthy is that which imposes a greater responsibility upon NRAs to ensure access and interconnectivity. Article 5 of the Directive delineates the powers and responsibilities of the NRAs concerning access and interconnection. This provision states that NRAs shall "*encourage and where appropriate ensure, in accordance with the provision of this Directive*, adequate access and interconnection, and interoperability of services, exercising their responsibility in a way that promotes efficiency, sustainable competition, and gives maximum benefit to end-users."[48]

Furthermore, Article 5(1)(a) "allows NRAs to impose obligations on undertakings that control access to end-users. . . to ensure end-to-end connectivity. . ."[49] This would apply to non-SMP

45. Access Directive, *supra* note 34, art. 2(c).

46. Communications Act, 2003, c. 21, § 32 (Eng.) [hereinafter "Communications Act"] *available at* http://www.opsi.gov.uk/acts/acts2003/pdf/ukpga_20030021_en.pdf.

47. *Id.* art. 2(a). Moreover the Council recognizes that,

> [t]he term 'access' has a wide range of meanings, and it is therefore necessary to define precisely how that term is used in this Directive, without prejudice to how it may be used in other community measures. An operator may own the underlying network or facilities or may rent some or all of them.

Id. recital 3.

48. Council Directive 2002/19/EC, *supra* note 34, art. 5, rule 3.3 (emphasis added).

49. OFTEL, GUIDANCE ISSUED BY THE DIRECTOR GENERAL OF

(significant market power) operators; a particular example given under recital 6 of the Directive is network operators that restrict end-user choice for access to Internet portals and services.[50] Although this is applicable to non-SMP operators, a greater emphasis is placed under the Directive on SMP operators. Consider Article 14(2) of the Framework Directive, which defines an SMP operator as one that

> either individually or jointly with others . . . enjoys a position equivalent to dominance, that is to say a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.[51]

This definition is closely aligned to the present case law of the European Court of Justice on what constitutes a dominant market position.[52] The Commission has also issued guidelines in assessing whether an operator has market power in the defined market.[53]

TELECOMMUNICATIONS, 11 (May 27, 2003), a*vailable at* http://www.ofcom.org.uk/static/archive/Oftel/publications/eu_directives/2003/endcon0503.pdf.

50. *Id.* recital 8. In the U.K., the Office of Telecommunications [hereinafter Ofcom] has published its latest statement. OFCOM, END-TO-END CONNECTIVITY (2006), http://www.ofcom.org.uk/consult/condocs/end_to_end/statement/statement.pdf.

51. Framework Directive, *supra* note 31, at art. 14(2).

52. *See, e.g.,* United Brands Co. v. Comm'n of the Eur. Cmties., Case 27/76, 1978 E.C.R. 207 (E.C.J. 1978); *see generally* DG INFSO, GUIDE TO THE CASE LAW OF THE EUROPEAN COURT OF JUSTICE IN THE FIELD OF TELECOMMUNICATIONS 16 (2003), http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/infringements/guidetocaselaw.pdf.

53. *See* Commission Guidelines on Market Analysis and the Assessment of Significant Market Power Under the Community Regulatory Framework for Electronic Communications Networks and Services, (EC) 2002/C165/03, July 11, 2002, 2002 O.J. (C 165) 6, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/c_165/c_16520020711en00060031.pdf. The Commission has recently published a draft recommendation in 2006 on a revised market definition. Commission Staff Working Document: Public Consultation on a Draft Recommendation On Relevant Product and Service Markets within the Electronic Communication Sector Susceptible to Ex Ante Regulation in Accordance with Directive 2002/21/EC of the European Parliament and of the Council on a Common Regulatory Framework for Electronic Communication Networks and Services, SEC(2006) 837, at 6, June 28, 2006, *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/recommendation_final.pdf.

If an operator is found to have SMP (at wholesale level),[54] then the NRA can, under the Interconnection and Access Directive, impose the following obligations:

- Transparency obligations (Article 9)
- Non-discrimination obligations (Article 10)
- Accounting separation obligations (Article 11)
- Obligations requiring mandatory access to be granted to specific network facilities (Article 12)
- Price control and cost accounting obligations (Article 13)[55]

The Interconnection and Access Directive clearly states under Article 8(4) that obligations imposed should be "*proportionate* and *justified* in the light of the objectives laid down in Article 8 [of the Framework Directive]."[56]

Article 12 is relevant because NRAs can impose obligations on operators to meet reasonable requests for access to, and use of, specific network elements. Examples provided under Article 12 include:

> (a) to give third parties access to specified network elements and/or facilities, including unbundled access to the local loop;
>
> (b) to negotiate in good faith with undertakings requesting access;
>
> (c) not to withdraw access to facilities already granted;
>
> (d) to provide specified services on a wholesale basis for resale by third parties;
>
> (e) to grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network services;
>
> (f) to provide co-location or other forms of facility sharing, including duct, building or mast sharing;
>
> (g) to provide specified services needed to ensure interoperability or end-to-end services to users, including facilities for intelligent network services or roaming on mobile

54. At the retail level, Articles 17-19 of the Universal Services Directive, *supra* note 35 would apply.

55. Access Directive 2002/19/EC, *supra* note 34, arts. 9-13.

56. *Id.* art. 8(4).

networks;

(h) to provide access to operational support systems or similar software systems necessary to ensure fair competition in the provision of services;

(i) to *interconnect networks or network facilities.*[57]

It is arguable that implicit within Article 12 is a network neutrality principle such that accessibility to networks is preserved. However, the only limitation is that it does not apply to non-SMP operators. For non-SMP operators, Article 5(1)(a) of the same Directive may come into play with NRAs, taking a greater responsibility to ensure connectivity to end-users. It is interesting to note the emphasis placed under the Directive upon NRAs to ensure that consumers are not disadvantaged if access-tiering should occur between network providers.

Furthermore, unlike in the United States, the broadband market in the United Kingdom is such that consumers can easily switch from one network operator to another,[58] and arguably, if a service has been downgraded by one network provider, consumers can always take the initiative and switch from one network operator to another, enabling consumers to change their service if it is downgraded by their current operator. In the latest report published by Ofcom,[59] approximately 69% of U.K. Internet users surveyed thought it would be easy to switch Internet service providers, and this is further reinforced by new rules introduced by Ofcom, which came into force on February 14, 2007 for broadband migrations between different Internet service providers.[60] Thus, even if network operators tried to discriminate between service providers, this is unlikely to sit well with consumers, who would likely switch providers.[61]

57. *Id.* art. 12 (emphasis added).

58. *See* OFCOM. THE COMMUNICATIONS MARKET: BROADBAND: DIGITAL PROGRESS REPORT 38 (2007), *available at* http://www.ofcom.org.uk/research/cm/broadband_rpt/broadband_rpt.pdf. In the United Kingdom, it was identified in the report that over a quarter (27%) of residential Internet users had changed service provider in the last quarter of 2006. *Id.* at 36.

59. *Id.*

60. *Id.*

61. *See* Access Directive, *supra* note 34, art. 5(1)(a), which enables NRAs to

Finally, one should also add that Regulation 2887/2000 on unbundled access to the local loop makes it mandatory for "notified operators" to meet reasonable requests for unbundled access to their local loop under "transparent, fair and non-discriminatory conditions."[62] It is only applicable to the traditional copper loop (last mile) and requires the notified operators to provide unbundled access to the local loop and related facilities (to be charged at cost-orientated prices as determined by NRAs). Access could only be refused on the basis of technical feasibility or the need to maintain network integrity.[63] "[T]he Regulation also requires the incumbent [operators] to offer shared access and sub-loop unbundling."[64] Shared access occurs when voice traffic would remain with the original supplier, while broadband access is provided by a new operator. The regulation underscores the E.U.'s commitment to liberalize the telecommunications market. In the E.U.'s European Electronic Communications Regulation and Markets 12th report, more than 4.1 million unbundled local loops were said to have been identified.[65] By opening the last mile to competitors, it would also prevent the monopolization that might occur with only a few incumbent operators and enhance consumer choice on broadband network providers.

At the time of writing, the European Commission indicated in a recent communication that it will monitor legal developments of network neutrality in the United States,[66] but it is unclear whether

impose obligations on undertakings that control access to end users to ensure end-to-end connectivity.

62. Regulation 2887/2000 of Dec. 18, 2000 on Unbundled Access to the Local Loop, 2000 O.J. (L336) 4, 7. *See also* Ofcom, *LLU Factsheet,* at http://www.ofcom.org.uk/static/archive/oftel/publications/broadband/dsl_facts/LLUbackground.htm (last visited Aug. 7, 2007).

63. See Commission Regulation 2887/2000, 2000 O.J. (L336) 4, art. 3.

64. Ofcom, *What is Local Loop Unbundling?* http://www.ofcom.org.uk/static/archive/oftel/publications/broadband/dsl_facts/LLUbackground.htm (last visited Apr. 4, 2008).

65. *European Electronic Communications Regulation and* Markets 2006, COM(07)(155) at 7, *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/12threport/sec_2007_403.pdf.

66. *See* Internet: Commission Seeks a Global Partnership on Internet Governance, Freedom of Expression and the Combat Against Cyber-repression, IP/06/542 (Apr. 27, 2006) *available at* http://ec.europa.eu/information_society/

anything will transpire on this front.[67] The prevailing view is that the existing European legislative framework is sufficient to deal with conflicts arising between network and cable providers and therefore, does not necessitate the types of regulations anticipated in the United States. [68] Arguably, it also reflects the apprehension existing in Europe with using *regulation* to dictate a particular path on network neutrality.[69] As one author commented:

> My biggest fear in this debate is that we don't know enough about the consequences to turn the Internet into a two-tier system. The E.U. is right to be neutral on neutrality. We're not ready to legislate.[70]

However, such feelings of apprehension seem to be misplaced because there is the regulation that exists at a European level under the new regulatory framework, which was discussed above.

Whether the existing regulation will be sufficient to deal with overt discrimination between broadband providers and application providers is unclear. One legal practitioner took the view that the existing legal framework will not be robust enough to prevent the types of discrimination that may arise in Europe.[71] Self-regulation is one option whereby content providers can aggregate and prevent broadband providers from discriminating, but no collective body at this stage presently exists. In the next section, we shall consider the U.K. framework in brief.

---

activities/internationalrel/docs/wsis/i06_542.en.pdf [hereinafter Commission Common Position]; Commission Press Release: EU Brokers Deal on Progressive Internationalisation of Internet Governance at Tunis World Summit, *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/1433&format=HTML&aged=0&language=EN&guiLanguage=en (last visited Apr. 4, 2008). *See also* Viviane Reding, *Content online: Europe's Strategy to Foster Content Creation and Distribution in the Multiplatform Media Business*, Address Before the Conference "creativity online.fi" [sic] (July 14, 2006), *available at* http://ec.europa.eu/commission_barroso/reding/docs/speeches/helsinki_content_online_20060714.pdf (last visited Apr. 4, 2008).

67. *See* Commission Common Position *supra* note 66.

68. *See* Ofcom, *supra* note 62.

69. *See* Victoria Shannon, *The End User: Neutrality? Yes or No*, INT'L HERALD TRIB., June 21, 2006, *available at* http://www.iht.com/articles/2006/06/21/business/ptend22.php.

70. *Id.*

71. Grateful acknowledgments to Paul Ganley, of Baker and Mackenzie, for his views.

B. United Kingdom: Communications Act 2003

The national regulatory authority in the United Kingdom, Ofcom,[72] took the view that the existing regulatory framework does not necessitate further rules on network neutrality, stating:

> One of the important principles underlying the way Ofcom regulates in the U.K. is that we have said we will act with a bias against intervention. That principle is important in the case of net neutrality because – were we to intervene if we were to follow the path suggested in the U.S. – we would be *dictating a new market structure* – a very dangerous place for a regulator to be.[73]

The echoes from Ofcom highlight the concerns over reasons why further regulation is not considered necessary.[74] The current E.U. and U.K. regulatory framework already provides for remedies against network operators that have significant market power (SMP) and charge for prioritization, blocking or degrading traffic. Such remedies, in Ofcom's view, include the obligation to supply, charge caps, and mandate ISPs. Ofcom does acknowledge that network neutrality rules "could be easily developed as an iteration of the existing non-discrimination rules."[75]

This goes back to an earlier point that the current European

72. *See e.g.,* OFCOM, THE COMMUNICATIONS MARKET *2006: 3 Telecommunications* (Aug. 10, 2006), at http://www.ofcom.org.uk/research/cm/cm06/telec.pdf; Ofcom Office of Communications, *Regulatory Challenges Posed by Next Generation Access Networks*, at http://www.ofcom.org.uk/research/telecoms/reports/nga/ nga.pdf (Nov. 23, 2006); For a background into the telecommunications industry in the U.K., *see* Paul Brisby, *The Regulation of Telecommunications Networks and Services in the United Kingdom*, 12 COMP. & TELECOM. L. REV. 114 (2006).

73. OFCOM, Joint CEPS and Progress for Freedom Conference, (Feb. 22, 2007), at http://www.ofcom.org.uk/media/speeches/2007/02/net_neutrality (emphasis added).

74. *See e.g.,* Richard O Levine & Randolph J. May, *Progress and Freedom Found: Interconnection Without Regulation: Lessons for Telecommunications Reform From Four Network Industries*, Oct. 2005, *available at* http://www.pff.org/issues-ubs/communications/books/051018Interconnection.pdf; Ofcom, *Review of the Wholesale Broadband Access Markets 2006/7*, http://www.ofcom.org.uk/ consult/condocs/wbamr/summary, (last visited July 20, 2007).

75. Tom Kiedrowski on behalf of David Currie, Joint CEPS and Progress for Freedom Conference (Feb. 22, 2007), *available at* http://www.ofcom.org.uk/media/speeches/2007/02/net_neutrality.

framework provides: a structure which would enable existing Internet service providers to operate and one in which the remedies are sufficient to deal with blocking of applications without having to resort to further legislative measures.

In the United Kingdom, the starting point is the Communications Act 2003[76] ("CA"), which implements the Access and Interconnection Directive. In particular, Part 2, Chapter 1 of the CA 2003 on electronic communications networks and services. Access is defined widely under § 151(3) of the Communications Act 2003 as:

> (a) interconnection of public electronic communications networks; or
>
> (b) any services, facilities or arrangements which-
>
> (i) are not comprised in interconnection; but
>
> (ii) are services, facilities or arrangements by means of which a communications provider or person making available associated facilities is able, for the purposes of the provision of an electronic communications service (whether by him or by another), to make use of anything mentioned in subsection (4);[77]

and references to providing network access include references to providing any such services, making available any such facilities or entering into any such arrangements.

Access to networks includes end-to-end communications service such as unbundled local loops and virtual network services.[78] The most recent case that considered interconnection is *British Telecommunications Plc v. Office of Communications* [79](formerly Director General of Telecommunications), which limited the definition of "interconnection" under the Access and Interconnection Directive to the connection of public

76. *See also* Notified Transposition Measures for Directive 2002/19/EC, *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/lirary/transportation/uk_2002_19.pdf (last visited Feb. 18, 2008).

77. Communications Act, *supra* note 46.

78. Ofcom, Imposing Access Obligations under the New EU Directives, *available at:* http://www.ofcom.org.uk/static/archive/oftel/publications/ind_guidelines/ cce0902.htm (last visited May 6, 2008).

79. [2004] CAT 8.

telecommunications networks for the purpose of achieving "end to end" interoperability and allowing the end user of one network to communicate with the end user of another. Therefore, the supply of circuits would not constitute "interconnection" within the Interconnection and Access Directive and the U.K. Regulations, 6(6).

In implementing the Access and Interconnection Directive, the main provision dealing with the imposition of obligations on SMP operators is in the Communications Act of 2003:

> (1) For the purposes of this Chapter a person shall be taken to have significant market power in relation to a market if he enjoys a position which amounts to or is equivalent to dominance of the market.
>
> (2) References in this section to dominance of a market must be construed in accordance with any applicable provisions of Article 14 of the Framework Directive.
>
> (3) A person is to be taken to enjoy a position of dominance of a market if he is one of a number of persons who enjoy such a position in combination with each other.
>
> (4) A person or combination of persons may also be taken to enjoy a position of dominance of a market by reason wholly or partly of his or their position in a closely related market if the links between the two markets allow the market power held in the closely related market to be used in a way that influences the other market so as to strengthen the position in the other market of that person or combination of persons.
>
> (5) The matters that must be taken into account in determining whether a combination of persons enjoys a position of dominance of a services market include, in particular, the matters set out in Annex II to the Framework Directive. This probably needs a citation.[80]

In particular, Section 151(2) defines interconnection as follows:

> . . .[R]eferences to the linking (whether directly or indirectly by physical or logical means, or by a combination of physical and logical means) of one public electronic communications network to *another for the purpose of enabling the persons using one of them to be able-*

80. Communications Act, *supra* note 46, §78.

(a) to communicate with users of the other one; or

(b) to make use of services provided by means of the other one (whether by the provider of that network or by another person. Again, probably needs a citation.[81]

Market power is elaborated under § 79 of the Communications Act of 2003, whereby Ofcom would have to identify the markets and carry out an analysis, taking into account the guidelines promulgated in by the European Commission.[82]

The question then is whether the U.K. Communications Act of 2003[83] can guarantee end-to-end connectivity for users. A useful example is to consider BT and Kingston. The director of Oftel has been able to impose obligations on BT and Kingston to provide network access on reasonable request to third parties and to do so "on fair and reasonable terms, conditions and charges" by virtue of Sections 151(3) and 151(4) Communications Act of 2003.[84] Furthermore, Ofcom was able to impose the following conditions on BT as provided under Section 12:

- requirement to publish a reference offer;
- requirement to notify terms and conditions;
- requirement to notify technical information;
- requirement to provide quality of service information;
- requirement to establish a statement of requirements for new

81. *Id*, § 151.

82. For the guidelines, *see generally* Commission Recommendation on 2003/311/EC L114/45, *available at* http://ec.europa.eu/information_society/ policy/ ecomm/doc/article_7/recom_11022003.pdf (last visited May 8, 2008); *see also* Commission Guidelines on Market Analysis and the Assessment of Significant Market Power under the Community regulatory framework for electronic communications networks and Services, 2002/C 165/03 *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/article_7/guidelines.pdf (last visited May 8, 2008).

83. Communications Act, *supra* note 46.

84. OFCOM, REVIEW OF THE FIXED NARROWBAND WHOLESALE EXCHANGE LINE, CALL ORIGINATION, CONVEYANCE AND TRANSIT MARKETS, 19 (2003), *available at* http://www.ofcom.org.uk/consult/condocs/narrowband_mkt_rvw/ nwe/fixednarrowbandstatement.pdf; *See also* OFFICE OF COMMUNICATIONS, REVIEW OF THE WHOLESALE BROADBAND ACCESS MARKETS, 101 (2004), *available at* http://www.ofcom.org.uk/consult/condocs/wbamp/wholesalebroadbandreview/ broadbandaccessreview.pdf.

access;

• requirement to have accounting separation.[85]

This is a classic illustration in which NRAs (Ofcom in this case) are able to ensure that connection between different networks is maintained and that SMP operators do not misuse their position.

The most recent example whereby the NRA has been able to impose obligations on non-SMP operators under the corresponding national provision to Article 5(1) of Access and Interconnection Directive is the case UK/2003/19 in which Ofcom notified Sky Subscriber Services Limited, the only provider of access control services for digital TV, of an obligation to provide access to these services on fair, reasonable and non-discriminatory terms.[86] Although Article 5(1) of the Access and Interconnective Directive may be exercised by Ofcom, this power is not always used.[87]

An example, whereby this power was exercised is the case, PL/2007/0631 concerning the dispute settlement regarding mobile access obligations in Poland.[88] In brief, the Polish national regulatory authority, ("UKE"), notified the European Commission about a draft dispute settlement decision which required the mobile network, ("PTC"), to provide mobile services to Tele 2.[89] As the parties did not reach an agreement, the United Kingdom decided to initiate a dispute settlement procedure on behalf of Tele 2, arguing that Articles 4(1) and 5(1) of the Access Directive enabled the NRA to impose access obligation to non-SMP operators for the

85 REVIEW OF THE FIXED NARROWBAND WHOLESALE EXCHANGE LINE. *supra* note 83, at 5.

86. OFCOM. CONDITIONAL ACCESS CHARGES – CONSENT IN RELATION TO NOTIFICATION REQUIREMENTS, para. 2.1, *available at* http://www.ofcom.org.uk/consult/condocs/accesscharges/statement/statement.pdf.

87. Interview with Tom Kiedrowski, Strategy Manager, Office of Telecomm., in London, Eng. (Jan. 18, 2008). The authors would like to thank Mr. Kiedrowski for providing his assistance through a series of informal discussions concerning network neutrality in the United Kingdom.

88. *See* Letter from Fabio Colasant, Director General, European Commission, to Anna Streżyńska, President, Urząd Komunikacji Elektronicznej [Polish national regulatory authority] (July 6, 2007), *available at* http://www.urtip.gov.pl/_gAllery/66/67/6667/uwagi_KE_konsultacje_MVNO_en.pdf (discussing Dispute settlement under article 5 of the Access Directive with regard to mobile access obligations in Poland).

89. *See id.* at 1.

purpose of the provision of mobile services.[90] It further contended that Article 5 of the Access Directive enabled NRAs to impose SMP-specific obligations on non-SMP operators.[91] The Commission, however, did not agree with the interpretation of the UKE and held that the power given to NARs under Article 5(1) was to: "encourage and where appropriate ensure, in accordance with the provisions of this Directive, adequate access and interconnection, and interoperability of services" was clearly limited by reference to "the objectives set out in Article 8 of Directive 2002/21/EC (Framework Directive)", to the need to "promote efficiency, sustainable competition and giving maximum benefits to end users."[92]

The Commission was of the view that the access obligations under Article 5(1) could not be imposed to hypothetical, future customers who would only exist after this obligation was imposed.[93] "Since Tele 2 is not yet operational as a mobile operator in Poland. . . , and therefore does not have any customers, an access obligation [could not] be justified on the grounds of the need for end-to-end connectivity or interoperability."[94] The European Commission's decision clarifies the application of Article 5(1) and access obligations.

Finally, Ofcom carried out a consultation which ended in December 2007[95] to investigate ways to develop the United Kingdom's existing telecommunications infrastructure. This consultation followed a recent press report from *The Times* stating that high bandwidth services such as Web TV (YouTube, BBC iPlayer for example) are likely to strain the telecommunications

90. *See id.* at 2.

91. *See id.*

92. *Id*. at 4.

93. *Id.*

94. *Id*.

95. *See* Ofcom, *Ofcom Considers Fast Broadband Outlook and Pledges Clarity for Investors,* Sept. 26, 2007, *available at* http://www.ofcom.org.uk/media/news/2007/09/nr_20070926; David Meyer, *Ofcom Launches Fibre-access Consultation,* ZDNET, (Sept. 26, 2007), *available at* http://news.zdnet.co.uk/communications/0,1000000085,39289650,00.htm. *See also* http://www.ofcom.org.uk/consult/condocs/nga/ for Ofcom's consultation paper. (last visited March 27, 2008).

infrastructure.[96] The consultation aimed to analyse the outlook for future broadband "Next Generation Access" (NGA) networks[97] with proposals for future regulation of this new communications infrastructure. One solution that Ofcom is exploring is whether utility companies can lay down fiber-optic cables (that would deliver these bandwidth services) as is happening in countries such as France.[98] These proposals are still in their premature stages, and no concrete plans are yet in place, but it indicates Ofcom's commitment to ensure that high bandwidth services are not affected by technical obstacles.[99]

In the context of proposed regulatory reform, Ofcom proposes two new principles. Namely, "regulation must reflect the significant commercial investment risk associated with deployment of these networks in order to ensure incentives for investment are retained"; and secondly, "investment in these networks requires regulatory clarity."[100] According to the Ofcom, "it is important that the regulatory regime remains in place for a sufficient time to allow investors the long-term clarity they need to invest with confidence." [101]

To conclude the European and U.K. section, the existing regulations under the Communication Act of 2003 and the Access and Interconnection Directive means that that scenario of access tiering between network operators and application providers may appear remote. If this practice were to occur, the NRAs have a responsibility to ensure end-to-end connectivity for non-SMP operators under Article 5(1) of the Access and Interconnection Directive or in the case of (wholesale) SMP operators, fulfill

96. *Id.*

97. *Ofcom considers fast broadband outlook and pledges clarity for investors,* (Sept. 26, 2007), http://www.ofcom.org.uk/media/news/2007/09/nr_20070926; *See also* http://www.ofcom.org.uk/consult/condocs/nga/summary/ for further details.

98. Jonathan Richards, *Web TV demands high-power broadband,* TIMESONLINE (Aug. 15, 2007), http://technology.timesonline.co.uk/tol/news/tech_and_web/article2265400.ece.

99. *Id.*

100. *Ofcom considers fast broadband outlook and pledges clarity for investors,* (September 26, 2007), http://www.ofcom.org.uk/media/news/2007/09/nr_20070926.

101. *Id.*

obligations as provided under this Directive.

IV. UNITED STATES: NETWORK NEUTRALITY

Network neutrality has become an issue of intense debate within the United States. The debate hinges on the fear that broadband companies will support certain content-based websites and not others, thereby influencing consumer actions. Regulation is necessary. Why? Today, as in 1934, telecommunication services were regulated in some fashion to protect the consumers from monopolies and to serve the public interest. Other federal regulations of telecommunication services served to ensure consumer rights to privacy. Today, verbal and written content traverse the same digital medium to transmit messages.

If Congress does not act and mandate network neutrality, it could end the existence of the Internet, because states that enact legislation could segregate the Internet by creating an Internet jurisdictional technology nightmare. In June of 2007, the state senate in Maine passed a bill that would require Internet Service Providers to ensure a non-discriminatory Internet.[102] Given the scope of this paper, the subject of Internet segregation will not be explored here.

Consequently, broadband providers that favor one Internet service over another may violate state network neutrality legislation, enacted by local, state, or Federal privacy law,[103] or specific statutes passed by State and Federal government to provide citizens with access to information.[104]

102. S.B. 580, 123rd Leg., (Me. 2007), *available at* http://www.mainelegislature.org/legis/bills/billpdfs/LD167501.pdf (last visited Apr. 14, 2008); *See* Nate Anderson, *Maine Waters Down, Passes Network Neutrality Resolution*, June 18, 2007, http://arstechnica.com/news.ars/post/20070618-maine-waters-down-passes-network-neutrality-resolution.html.

103. *See* M.J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?* 19 JOURNAL OF PUBLIC POLICY AND MARKETING 1, 20-26 (2000).

104. *See* MEGHAN E. COOK, CENTER FOR TECHNOLOGY IN GOVERNMENT, UNIVERSITY AT ALBANY, SUNY, WHAT CITIZENS WANT FROM E-GOVERNMENT: CURRENT PRACTICE RESEARCH, (2000), *available at* http://www.ctg.albany.edu/publications/reports/what_citizens_want/what_citizens_want.pdf; *See also* Sandford Borins, *On the Frontiers of Electronic Governance: A Report on the United States and Canada*. 68 INT'L REV. OF ADMINISTRATIVE SCIENCES 2, 199-211 (2003); Andrew Chadwick and Christopher May.,

For example, broadband company ABC enters into a contract with *xTV,* where *xTV* is the only broadband Search, TV, and phone service. ABC consumers can access the Internet, but are not able to access *jTV* via the Internet, even though *j*TV provides cheaper TV and phone service. This scenario raises several issues (not exhaustive):

Privacy: The broadband provider would need to monitor a consumer's Internet usage and block the consumer's use of *jTV* Internet service and re-direct them to *xTV* (violating their privacy rights).

Access to Government Information: The broadband provider by limiting the consumer to only *xTV* may be limiting the consumer's ability to access information because it is foreseeable that *xTV* does not provide consumers access to crucial government information that is provided only online (Only on TV?).

E911: Access to certain crucial phone services, such as 911, because *xTV* determined that such services were not cost effective.

These scenarios demonstrate the public policy reasons that the government should pass legislation that mandating network neutrality.

A counter-argument to the need for regulation is that consumers will transform their buying patterns so their broadband providers carry the content. But should economic wealth determine whether one can phone 911 or read about local or national legislation or watch political debates?

This contention, however, is inaccurate. Unlike in the past, content providers are now tending to offer a full range of communications products, often bundled together. The question is, how can a consumer migrate to a cost-effective broadband provider if choices are limited or impossible? And certainly, broadband carriers should block competitors who seek to deliver phone or cable services using their bandwidth. Otherwise, the broadband companies are simply giving competitors a free ride. Even if technology allowing the circumvention of the Internet, cable, and

Interaction between States and Citizens in the Age of the Internet: "E-Government" in the United States, Britain, and the European Union 16 GOVERNANCE: AN INTERNATIONAL JOURNAL OF POLICY, ADMINISTRATION, AND INSTITUTIONS 2, 271-300 (2003).

phone trifecta existed, the question remains how the consumer would learn about the technology. A broadband provider could simply restrict the consumer from reading about the company from their website, seeing the company's advertisements on cable, or receiving direct e-mails from the company itself.

Broadband technologies control the proverbial marketing spigot, thereby making the costs to enter the market astronomical and also making investment in such technologies a money losing proposition. Even if the counterargument of market competition is valid, the technology precepts to execute broadband content discrimination potentially infringe upon the constitutional and federally recognized right to privacy for oral communications in the home.[105]

Finally, the network neutrality debate fails to consider the potentially costly outcome if broadband discrimination is permitted without network neutrality; namely the exodus of website content providers from the United States to more favorable countries. Internet application companies, in an effort to avoid broadband discrimination, might choose to relocate to a country where network neutrality is guaranteed by law. While this is not the case today, if the U.S. Congress does not regulate broadband and ensure network neutrality, significant damage may be done to the United States' position as a global leader in technology.

A. Current U.S. Framework on Network Neutrality

The Telecommunications Act of 1996 (the "1996 Act")[106] is the first major legislation addressing telecommunications since the original Communications Act of 1934[107] (the "1934 Act") was intended to address a new era in communications, and to serve as a framework for regulating emerging technologies and markets. Two significant principles are evident in the Act: the conviction that any new regulatory model must ensure competition, and the belief that it is necessary to promote universal access to advanced and

105. *Id*.

106. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in 47 U.S.C.S. § 151 et seq).

107. *See id*.

affordable communication.[108]

A significant aspect of the 1996 Act is the distinction it makes between providers of "telecommunications services" and "information services."[109] Under the 1934 Act, as amended by the 1996 Act, the term "telecommunications service" was defined as the "offering of telecommunications for a fee directly to the public . . . regardless of the facilities used."[110] The 1934 Act further defined telecommunications as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[111] Next, it defined "telecommunications carrier[s]" - those subjected to mandatory Title II common-carrier regulation - as "provider[s] of telecommunications services[.]"[112] Finally, the term "information service" was defined as the "offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[113]

Carriers selling broadband Internet access, pursuant to recent Supreme Court decisions discussed infra, are considered information services carriers.[114] It is here where the distinction is important. The 1996 Act regulates telecommunication carriers, while information service carriers do not fall under its purview.[115] Consequently, a carrier providing information services is not a "telecommunications carrier" under the 1996 Act, thereby precluding its applicability.[116] The area of communications is dynamic. As advancing technologies have converged and become interconnected, the level of competition has increased. Traditionally distinct service providers, such as cable television and telephone service providers, now find themselves in direct

108. *Id.*
109. 47 U.S.C.S § 151 et. seq.
110. *Id.* § 153(46).
111. *Id.* § 153(43).
112. *Id.* § 153(44).
113. *Id.* § 153(20).
114. *See* texts accompanying *infra* notes 127 and 145.
115. *See* 47 U.S.C.S. § 153(44).
116. *Id.*

competition. Not surprisingly, the Courts have played a significant role in these new conflicts.

"The Supreme Court's decision in [*National Cable & Telecommunications Ass'n v. Brand X Internet Services*[117] [hereinafter "Brand X"] in June 2005 held that content and applications providers could no longer count on regulation to guarantee access to cable modem and DSL systems."[118]

In 2002, the Federal Communications Commission (FCC) declared that broadband cable modem service, specifically cable modem service and Digitial Subscriber Line (DSL) service was an information service, thereby precluding the applicability of the Title II common-carrier regulation.[119] The Ninth Circuit Court vacated the FCC ruling that cable modem service was not a telecommunications service under the 1934 Act.[120]

The Supreme Court on *certiorari* reversed and remanded the Ninth Circuit Court holding.[121] The court reviewed and upheld the FCC's decision to categorize broadband information carriers as Information Service Carriers as, thereby essentially granting them immunity from the applicability of Title II of the Communications Act of 1934 common-carrier regulation.[122] Justice Thomas wrote that "consumers used the high-speed wire always in connection with the information-processing capabilities provided by Internet access, and the transmission was a necessary Internet access component."[123] He further reasoned that

> what cable companies providing cable modem service and telephone companies providing telephone service 'offer' is Internet service and telephone service respectively - as finished services, though they did so using the discrete components composing the end product, including data transmission. Such

117. 545 U.S. 967 (2005).

118. Status Register, CHAMPAIGN-URBANA COMPUTER USERS GROUP Jan. 2007, http://www.cucug.org/sr/sr0701.html. "One indirect consequence of this was that companies such as Google, Microsoft, Earthlink and Intel began pouring money into wireless broadband and Broadband Over Powerline (BPL)[.]" *Id.*

119. Brand X Internet Servs. v. FCC, 345 F.3d 1120, 1123 (9th Cir. 2003).

120. *Id.* at 1132.

121. *Brand X*, 545 U.S. at 980.

122. *Id.*

123. *Id.*

> functionally integrated components did not need to be described as distinct "offerings."[124]

A broadband cable modem Internet service can manipulate and store information, and is thus an "information service" according to an FCC declaratory ruling; however, "the integrated nature of Internet access and the high-speed wire used to provide Internet access" led the FCC to the conclusion that a broadband cable modem services is not a "telecommunications service."[125] The ruling meant that common-carrier regulations did not apply to broadband cable modem services.[126]

The Supreme Court in *Verizon Communications Inc. v Law Office of Curtis V. Trinko* held that Respondent law firm's complaint alleging a breach of an incumbent local exchange carrier's (LEC) duty under the 1996 Act to share its network, failed to state a claim under §2 of the Sherman Act.[127] In *Verizon*, the Supreme Court explored whether Verizon had violated §2 of the Sherman Act by comparing the 1996 Act with the anti-trust principles of the Sherman Act [128] At issue was the 1996 Act's requirement that an incumbent LEC share its network with competitors. Specifically, the incumbent LEC must share its individual network elements without imposing any "bundling" requirements.[129] Verizon, as the incumbent LEC, signed interconnection agreements with rival LECs pursuant to the 1996 Act.[130] Verizon's competitors however, lodged complaints that Verizon violated these interconnection agreements. As a result, both the New York Public Service Commission (PSC) and the Federal Communication Commission (FCC) launched investigations into Verizon's practices.[131] These investigations led to a levying of financial penalties against Verizon, remediation

124. *Id.*

125. *Id*. at 977-78.

126. *Id* at 978.

127. *See Verizon Comm. v. Law Offices of Curtis V. Trinko,* 540 U.S. 398, 409-10 (2004).

128. *Id.* at 398.

129. *Id.* at 402.

130. *Id.*

131. *Verizon,* 540 U.S. at 398.

measures, and the imposition of further reporting requirements.[132] Subsequently, the Respondent, a telephone service customer of AT&T, a Verizon competitor, alleged that Verizon had engaged in discriminatory practices in filling the orders of its rivals, thereby violating the Sherman Act.[133]

The Supreme Court rejected this argument, holding that Respondent failed to state a claim under the Sherman Act because the 1996 Act did not conflict with traditional antitrust principles.[134] The Court reasoned that the 1996 Act does not expand applicability of the Sherman Act.[135] Additionally, the Court found that Verizon's previous violations did not constitute a claim under traditional antitrust standards.[136] Finally, the Court rejected the argument that the claim at issue should be identified as one of the limited exceptions to the general rule that there is no duty to help competitors.[137]

In Brand X Services, the Supreme Court overruled the Ninth Circuit, holding that the FCC was within its statutory rights to classify cable as an information service and therefore exclude cable companies from common carrier regulation.[138] The Commission later ruled that DSL was also an information service.[139] Thanks to this reclassification, DSL carriers are no longer subject to the requirement that they share DSL lines with broadband competitors.[140] Collectively, these decisions re-ignited the network neutrality debate.

B. Network Neutrality and Oral communications

The network neutrality debate focuses on whether last-mile providers are blocking access to content and applications. Network

132. *Id.*
133. *Id.*
134. *See id.* 540 U.S. at 411.
135. *Id.*
136. *Id.* at 415-16.
137. *Id.* at 411.
138. *See* 545 U.S. 967, 987 (2005).
139. *Id.* at 978.
140. Bill D. Herman, *Opening Bottlenecks: On Behalf of Mandated Network Neutrality*, 59 FED. COMM. L.J. 108, 131 (2006).

neutrality assures that infrastrucure does not distinguish content when delivering information. Network service providers do not affect the delivery of data based on their content. Today, network neutrality is effectively non-existent.

Leading broadband companies argue that they have not blocked access to content or applications and that market forces prevent them from doing so in the future.[141] This market argument is erroneous because broadband service providers (BSPs) are effectively preventing consumers from accessing an array of Internet applications and from creating a tiered Internet by granting preferential treatment to application and content providers that compensate BSPs monetarily.[142] Proponents of legislation enforcing meaningful network neutrality assert that failing to legislate will result in (1) BSPs use of discriminatory access arrangements that harm competition and consumers, and (2) the formation of a tiered Internet caused by BSPs prioritizing traffic on their networks, allowing BSPs to charge application and content providers for higher quality of service to access BSPs' networks. [143]

What is missing from this debate is a discussion of the issue of privacy. Network neutrality ties into the privacy of oral communication since the Internet today delivers telecommunication services to consumers that select from an expansive set of application sets. Therefore, the issue is whether a BSP can monitor a consumer's oral communications in such a way that creates the most favored Internet application service. For example, a mother in Seattle using Google Chat can talk (meaning convey and receive oral communications) with a third party, who in this case is her son studying in graduate school in Boston. These oral communications receive protection from state and federal legal frameworks. Therefore, the BSP actions of monitoring and reviewing these Google Chat packets in determining whether those packets receive

141. *Id.*

142. *See* Tripp Blatz, *Three Carriers Have Now Blocked Access to Ports for VoIP, Vonage Chairman Alleges*, TELECOMM. MONITOR, Aug. 23, 2005.

143. *See* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. 41 (2003); Tim Wu, *Wireless Net Neutrality: Cellular Carterfone on Mobile Networks*, (New American Foundation Wireless Future Program, Working Paper, No. 11); *See also, Save the Internet,* at http://savetheinternet.com, (last visited Apr. 10, 2008).

the BSP's most favored Internet application service may be in violation of federal, state, and local laws protecting a citizen's oral communications.

Within the United States, oral communications receive protection from the legislative and judicial branches. Justice Brandeis "anticipated that technological advancement will enable the Government to employ tools of surveillance extending beyond wiretapping"[144] in *Olmstead v. United States*.[145] In that dissenting opinion, Justice Brandeis:

> asserted that Fourth Amendment protections must be interpreted broadly so as 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.[146]

Justice Brandeis' forward-looking focus on a person's underlying privacy interests presents a more compelling perspective than the premise of the Wiretap Act as currently applied by the courts.[147] Since *Katz v. United States*,[148] courts have routinely forbidden third parties from tapping or monitoring oral communications.[149] However, businesses routinely 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. [150]

144. Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email,* 10 MICH. TELECOMM. & TECH. L. REV. 1, 93 (2003).

145. 277 U.S. 438, 466, 472-74, 478 (1928) (Brandeis, J., dissenting).

146. Pikowsky, *supra* note 144; *see also Olmstead*, 277 U.S. at 472-74, 478-79.

147. *See Olmstead,* 277 U.S. 438, 472-74, 478-79.

148. 389 U.S. 347 (1967).

149. *See e.g.,* Simpson v. Simpson, 490 F.2d 803, 805 (5th Cir. 1974) (stating that the Omnibus Crime Control and Safe Streets Act "prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers") (quoting Senate Judiciary Comm., Senate Report No. 1097, 1968 U.S.C.C.A.N., 2153); Pritchard v. Pritchard, 732 F.2d 372 (4th Cir. 1984) (prohibiting unconsented wiretapping between spouses);

150. *See generally* Daniel B. Garrie, et.al., *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected*?, 29 SEATTLE U. L. REV. 97 (2005).

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.[151]

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.[152] The counterargument that "VoIP is clearly not your father's telephone service"[153] is not relevant to the issue of the citizens' right to telecommunication privacy. The main reason for this is that VoIP still transmits oral communications despite the fact it may not be "my father's telephone service."[154]

The courts have found telephone communications protected from governmental privacy invasions in two principal ways.[155] First, parties to a voice conversation are entitled to a "reasonable expectation of privacy" under the Supreme Court opinion of *Katz v. United States*.[156] Second, the Federal Wiretap Act of 1968 prevents unauthorized third-party interceptions of telephone communications, unless (1) the interceptor is in possession of a court order or (2) either of the involved parties in the communication has provided their consent.[157] The *Katz* opinion explains the rationale behind the Supreme Court's oft-quoted statement that the Fourth Amendment "protects people, not places,"[158] and concludes that an entity's reasonable expectation of

151. *See id.* at 100-01.

152. *Id.*at 101.

153. *In re* Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, 19 F.C.C.R. 7457, 7475 (2004) [hereinafter AT&T] (statement of FCC Chairman Michael K. Powell).

154. While it is not within the scope of this paper to address this argument further, the technology and the English language on which the law is based do not support the assertion that VoIP is an information service and not a telecommunication service, even though VoIP may act like a telecommunication service on steroids.

155. *See* Frierson v. Goetz, 227 F. Supp. 2d 889, 896-97 (M.D. Tenn. 2002) (describing a two-part test for determining qualified immunity).

156. *See* 389 U.S. at 350.

157. *See e.g.*, 18 U.S.C. §§ 2510-21 (2000).

158. *See Katz*, 389 U.S. at 351.

privacy must be protected from government searches.[159] The Federal Wiretap Act was Congress' response to the *Katz* opinion and was an attempt to prevent electronic surveillance of oral telephone communications without a court order. [160]

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.[161] *Katz* stands for the proposition that an individual can control what information about him and his actions is made available to the public,[162]and what remains private and protected by the Fourth Amendment.[163] The *Katz* doctrine of Fourth Amendment protections has a requires "first that a person have exhibited an actual (subjective expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[164] The courts have read *Katz* narrowly in recent years,[165] but because the Fourth Amendment's privacy protections only insulate individuals from governmental privacy encroachments,[166] the Wiretap Act is the

159. *Id.* 389 U.S. at 353 (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 with respect to wiretapping will be interpreted by the Supreme Court in the context of National Security interplaying with the constitutionally granted rights of the executive privilege.

160. *See* United States v. Andonian, 735 F. Supp. 1469, 1471 (C.D. Cal. 1990); S. REP. NO. 90-1097, at 66-72 (1968); 1968 U.S.C.C.A.N. 2110, 2153-59.

161. *See Katz,* 389 U.S. at 351.

162. *See id*. ("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.") (citations omitted).

163. *Id*. at 352.

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

165. *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 . . . When 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.

166. *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (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,

main cause of action protecting telephone communicants from non-governmental third-party interceptors.[167] Telephone communicants can obtain redress under the Wiretap Act for unauthorized third party interceptions of telephone communications unless the interceptor has a court order, a certification by the United States Attorney General or his or her agent that none is required,[168] or the consent of either party involved in the conversation.[169]

In summary, the Wiretap Act[170] initially afforded extensive protection to wire communications, but oral communications were protected only when there was a reasonable expectation of privacy.[171] Because the legislation covered both face-to-face oral communications and traditional point-to-point wired communications, courts were faced with myriad interpretive difficulties.[172] To correct the problems with Title III, Congress amended the Wiretap Act by passing the Electronic Communications Privacy Act of 1986 (ECPA).[173] Congress designed the ECPA to prohibit the intentional interception of oral, wire, and electronic communications.[174] Because Congress was concerned with advancements in electronic technology that would be capable of defeating any privacy expectations,[175] the ECPA

the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government"); Schmerber v. California, 384 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.").

167. *See* 18 U.S.C. §§ 2510-2521 (2004).

168. 18 U.S.C. § 2511(2)(a)(ii) (2004).

169. 18 U.S.C. § 2511(2)(d) (2004).

170. Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 212 (1968).

171. *See* 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 standard for determining when a reasonable expectation of privacy exists).

172. *See* 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).

173. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C. (1986)).

174. *See* S. REP. NO. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555-57.

175. *Id.* at 3555.

enacted a strict set of standards for the interception of oral, wire, and electronic communications. [176] Congress further expanded the protection of wireless communication by passing the Communications Assistance for Law Enforcement Act of 1994 (CALEA),[177] 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").[178] 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 about what protections are extended to VoIP oral communications.[179]

While the U.S. courts forbid third parties to tap or monitor oral telephone communications,[180] they routinely permit data packets[181] to be tracked, stored, and sold by third parties with the implied[182] or explicit[183] consent of either party engaged in the transmission. In the digital age, however, the law-made distinction between voice and data has become muddled. With the convergence of oral and data communications into a single transmission medium, the courts are unable to distinguish between oral telephone and electronic communications.[184] The use of VoIP and other broadband

176. 18 U.S.C. § 2518 (2004).

177. Pub. L. No. 103-414, §§202(a), 203, 108 Stat. 4279, 4290-91 (1994) (amending 18 U.S.C. § 2510 (2004)).

178. Pub. L. No. 107-56, 115 Stat. 272 (2001).

179. The scope and impact of the Patriot Act is beyond the scope of this paper. *See* John P. Elwood, *Prosecuting the War on Terrorism: The Government's Position on Attorney-Client Monitoring, Detainees, and Military Tribunals*, 17 CRIM. JUST. 30 (2002).

180. *See supra* note 149.

181. *See* Vonage Holdings Corp. v. Minn. Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 994 (D. Minn. 2003) (stating that the "Congress also differentiated between 'telecommunications services,' which may be regulated, and 'information services,' which like the Internet, may not").

182. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510 (S.D.N.Y. 2001); In re Toys R Us Inc Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *3 (N.D.Cal. Oct 09, 2001); Register.Com, Inc. v. Verio, Inc., 356 F.3d 393, 403 (2nd Cir. 2004).

183. *See In re* Pharmatrak, Inc., 329 F.3d 9, 19-22 (1st Cir. 2003).

184. *See Vonage*, 290 F. Supp. 2d at 1000-03.

communication technologies has made this legal distinction impossible to uphold because oral telephone and electronic data communications now travel over the same wires simultaneously, encapsulated in digital data packets.[185]

VoIP is a technology for transmitting ordinary telephone calls over the Internet.[186] "In other words, VoIP can send voice, fax and other information over the Internet, rather than through the PSTN (Public Switched Telephone Network) or regular telephone network."[187] For example, if you are connected to the Internet, you can simultaneously exchange data, audio or video with anyone while using VoIP, which is impossible with a regular telephone line.[188] This convergence of separate mediums shifts the legal landscape of digital communications[189] and requires further examination. This examination must proceed in light of the disparity in judicial treatment between oral telephone and electronic data communications, with oral telephone communications generally receiving a higher level of privacy protection.[190]

VoIP is no longer a fledgling technology;[191] it is rapidly

185. *See* FROST & SULLIVAN, VOIP EQUIP 2003 WORLD UPDATE (2003) (stating that companies selling IP telephony equipment generated more than $1 billion in revenues in 2000 and expect those revenues to exceed $14 billion by 2006).

186. *See* VoIP Consumer Facts, *supra* note 17.

187. Office of the Privacy Comm'r, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, 239, n.212 (2005) (Austl.) *available at* http://www.privacy.gov.au/act/review/revreport.pdf; *see also Vonage*, 290 F. Supp. 2d at 995.

188. *See* FROST & SULLIVAN, *supra* note 185.

189. *See generally,* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998).

190. *Compare Katz*, 389 U.S. at 353 (holding that electronically listening to telephone conversations "constitute[s] 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) (stating 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").

191. *See* Peter Grant, *Office Technology - Ready for Prime Time: A New Internet-Based Phone Technology Has an Un-Catchy Acronym: VoIP; But Don't Be Fooled: It Could Make Dramatic Changes in the Way Businesses Operate*, WALL ST. J., Jan. 12, 2004, at R7. Growth projections for VoIP vary widely, but the Wall Street Journal reported in early 2004:

> [b]y the end of this year, about 20% of the new phones being shipped to

becoming a mainstream communication product along with several other broadband communication technologies.[192] Both corporate and individual consumers are using VoIP to reduce their phone bills by capitalizing on their existing connections to Internet broadband infrastructure. [193] For example, Nissan North America, based in California, is implementing VoIP globally,[194] though dollar cost savings are not the only factor driving this decision.[195] Nissan and a multitude of other companies are utilizing VoIP to facilitate global communication between their offices because VoIP offers improved functionality over traditional telephone systems.[196] While large corporations that purchase VoIP systems to improve functionality and decrease costs[197] receive the primary benefit from these services, individual consumers also benefit from using VoIP that offers less expensive long distance and local phone services via their own home broadband Internet connections.[198]

> 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.

192. *See* FROST & SULLIVAN, *supra* note 185.

193. According to PC Magazine, "VoIP can save small businesses significant amounts of money, averaging about 30 percent on phone costs." Both large and small companies can save on communicating with their teleworkers or partners, even if they are working from another country, by placing the calls over the Internet. C. Wolter, *VoIP: The Right Call*, PC MAGAZINE, June 22, 2004, at 139, *available at* http://www.olmec.com/PC%20MAGAZINE%20VOIP%20ARTICLE.pdf.

194. *See* Stan Gibson, *VoIP Passes Nissan Road Test*, EWEEK, Jan. 24, 2005, at 32, 32.

195. *Id*.

196. *Id*. *See also* Wolter, *supra* note 193, at 139.

197. *See* CISCO SYSTEMS, INC., THE STRATEGIC AND FINANCIAL JUSTIFICATIONS FOR IP COMMUNICATIONS 2 (2001), *available at* http://www.interactiveusa.com/manager/uploads/cnvrg_wp.pdf. *See also,* Kevin Tolly, *VoIP: Neither Panacea Nor Pariah*, NETWORKWORLD, Feb. 18, 2002, at 24, *available at* http://www.networkworld.com/columnists/2002/0218tolly.html.

198. *See* Press Release, Infonet, Infonet Introduces Software Tool to Demonstrate ROI for Converged Networks (Nov. 13, 2001), *available at* http://www.bt.infonet.com/about/newsroom/press_release.asp?month=1113&year=2001. This software tool allows clients to evaluate their savings from installing VoIP system up-front, leading to faster adoption of VoIP technology. *Id*.

VoIP cost savings[199] arise from the ability to transmit oral and data communications simultaneously over the same medium, thereby eliminating the need for multiple phone and data lines in a home[200] or business.[201] VoIP technology threatens to break the oral communication monopolies held by the regional Bell companies because it eliminates the need for consumers to pay non-competitive fees to use a telephone line to carry oral telephone conversations.[202] VoIP transmits oral communications via Internet Protocol (IP) instead of the PSTN. [203] Unlike the PSTN,[204] VoIP is unlikely to face legal issues of monopolization and significant government regulation because multiple technologies such as satellite, wireless, cable, DSL, and IP over power line technology compete to be the communication service provider.[205]

While the market's invisible hand has already fostered technical innovations making some VoIP services superior to those offered by the traditional PSTN,[206] the legislature and the courts have yet to resolve two primary legal issues that are likely to hinder the United States' adoption of VoIP as the new oral communication standard. First, VoIP will have to contend with the extension of Congressional legislation from the PSTN to VoIP carriers[207] to tax

199. Paul Taylor & Peter Thal Larsen, *TIME WARNER CABLE Plans Big Push Into Internet-Based Phone Services*, FIN. TIMES, Dec. 9, 2003, at A1.

200. *See* Peter Grant, *Here Comes Cable. . .and it wants a big piece of the residential phone market*, WALL ST. J. Sept. 13, 2004 at R4.

> By the end of 2006, more than half of all 110 million-odd households in the U.S. will likely have the option of getting phone service from their cable companies. By 2008, cable companies will be selling phone service to 17.5 million subscribers, compared with 2.8 million at the end of 2003, according to an estimate by research firm Yankee Group.

201. *See* Gibson, *supra* note 194, at 34.

202. Grant, *supra* note 200.

203. *Id.*

204. *See* Yochai Benkler, Communications Infrastructure Regulation and the Distribution of Control over Content, 22 TELECOMM. POL'Y 3, 190-91 (1998).

205. *See* Grant, *supra* note 200.

206. For example, VoIP offers improved conference calling, combining e-mail and voicemail messages, portability and forwarding services, as well as transmission of fax and video data. *See, e.g.,* Grant, *supra* note 200 ; *see also* Wolter, *supra* note 193, at 141-142.

207. The Telecommunications Act of 1996 defines two important categories: "Telecommunications Services," which are subject to mandatory Title II regulation are defined in 47 U.S.C. §153(20) (1997), and 47 U.S.C. § 153(46)

the transmission of data and to regulate communication networks and line monopolies.[208] Second, the degree of privacy, if any, that the law will afford to VoIP oral communications must be defined.[209] The taxation issue lies entirely in the hands of a

(1997) defines "Information Services," which are exempt from such regulation *See* Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Serv., 545 U.S. 967, 975 (2005). The regulatory classification of a service is of extreme importance to incumbents and new entrants. For example, the Supreme Court recently upheld the FCC's initial classification of cable modem service as an information service, *In re* Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798, 4821–22, (2002), while classifying DSL as a telecomm. service. *In re* Deployment of Wireline Services Offering Advanced Telecomm. Capability, 13 F.C.C.R. 24011, 24030–31 (1998). *See generally*, *Brand X*, 545 U.S. 967 (2005). The Court reached this decision by agreeing that the F.C.C's cable modem regulation was reasonable, *id*. at 985, after applying the second step in the *Chevron* test. *Id*. at 986. To assess reasonableness, the Court examined the attributes of an information service under 47 U.S.C. § 153(20) (2004) (generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making information available via telecommunications—in this case, browsing the Web to transfer files via FTP and to access e-mail) vis-à-vis those of a telecommunication service under 47 U.S.C. § 153(43) (2004) ("the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received"). *Id.* at 987-88.

Strikingly, VoIP contains attributes of both an information service and a telecommunication service. The VoIP "stack" certainly stores, transforms, and converts information via telecommunications, so it is an information service. *See* Phillip Carden, *Building Voice Over IP*, NETWORK COMPUTING, May 8, 2000. But the purpose of all this storing, transforming, and converting is really to transparently transmit voice information to and from a user and another point of his choosing, all the while minimizing observable differences in the form or content of the information. VoIP providers are graded on how closely they emulate POTS. *See* Sam Schechner, *Smooth Operators: Which Internet Phone Service Is Best?*, SLATE MAGAZINE, June 29, 2005, http://slate.com/id/2121742 .

Whether VoIP services will be classified as a telecommunications service will eventually depend on whether the FCC considers VoIP a transparent transmission of information. *See Brand X*, 545 U.S. at 998-99. Note that the FCC did not consider cable modem service to be "transparent" because cable modem service includes DNS resolution and caching. *Id*. at 993.

208. *See generally* Declan McCullagh, *Congress Proposes Tax on All Net, Data Connections*, CNET NEWS, Jan. 28, 2005, http://www.news.com/Congress-proposes-tax-on-all-Net,-data-connections/2100-1028_3-5555385.html.
Congress's decisions to tax and regulate VoIP technology are beyond the scope of this paper.

209. *See e.g., Katz*, 389 U.S. at 353 (noting the use of electronic eavesdropping equipment overhear conversation inside telephone booth intrudes on legitimate expectation of privacy).

legislature that is actively attempting to extend PSTN taxation to IP communications networks.[210]

Under the current legal framework, unauthorized third-party access to oral telephone communications constitutes an invasion of any non-consenting person's privacy.[211] Courts will probably extend these privacy rights to VoIP communications as just another form of protected oral communication. Because VoIP oral communications are physically transmitted in the form of digital data packets over the Internet[212] and are essentially indistinguishable from Internet data communications, they should be legally protected by a constitutional right of privacy preventing third parties from tracking, tapping, storing or selling the communications.[213] VoIP opens a paradigm of oral privacy, which will place a considerable strain on the existing judicial canons protecting oral and data communications.[214] This legal privacy dichotomy poses a substantial risk that parties legitimately monitoring Internet data streams will unlawfully monitor constitutionally protected private VoIP communications.[215] It remains to be seen whether this strain will be severe enough to force courts to extend the same Constitutional privacy right to data communications that currently exists for oral communications.

If broadband companies triumph and a tiered Internet solution arises, these telecommunication/broadband companies will, in

210. *See generally* McCullagh, *supra* note 208.

211. *See* 18 U.S.C. § 2511(1) (2000) (Prohibiting the interception of oral of electronic communication).

212. *See Vonage*, 290 F. Supp. 2d at 1000-03 (finding that "Congress also differentiated between 'telecommunications services,' which may be regulated, and 'information services,' which like the Internet, may not").

213. Although courts have not had the opportunity to decide whether there is an expectation of privacy for data packets transmitted over the Internet, it is likely that given the opportunity, a court will. *See e.g.* Bartnicki v. Voppe, 532 U.S. 514 (2001) (finding that interception of cell phone conversations, which are transmitted as electronic packets, infringed on the defendant's privacy).

214. *See Katz*, 389 U.S. 347; *In re* Pharmatrak, 329 F.3d 9 (1st Cir. 2003); *Bartnicki*, 532 U.S. 514.

215. *See In re* Pharmatrak, Inc., 329 F.3d at 12 (holding that a third-party data mining company had explicit consent to monitor non-personally identifiable information, but did not have explicit consent to monitor personally identifiable information, such as social security number, last name, phone number, and date of birth).

varying degrees, monitor and intercept digital packets. In this case, where these digital packets contain oral communications transmitted using VoIP, or an Internet oral communication service, then the broadband company violates the judicially established privacy rights analyzed above. While the outcome is certainly unknown, it is foreseeable that the judicial, legislative, and executive branches, will address the issue of network neutrality with respect to privacy.

C. Oral Communications Delivered Over Municipal Broadband and Broadband Power Line Companies Entitled to a Higher Level of Privacy, Mandating State Adoption of Network Neutrality

If the legal points discussed above are resolved for private broadband ISP, the issue of state-funded municipal broadband ISPs will remain unanswered. Since the state would be the provider of broadband ISP services, there is a greater duty to protect citizens' right to privacy and provide citizens with unfettered access to information.[216] Arguably, a municipal broadband ISP that does not enforce the precepts of network neutrality, whether they violate federal or state privacy rights, exposes itself to legal suit.

Municipal broadband ISP providers that operate in certain states, which explicitly recognize a citizen's right to privacy (e.g., California),[217] require any municipal broadband ISP provider[218] within that state to enforce the precepts of network neutrality. The reason is that these specific ISPs cannot monitor a citizen's Internet usage without cause, due to the states' constitutions. Since a Broadband provider is unable to monitor a user's website access, they cannot charge website providers such as Google. They cannot prove that specific users accessed Google via their network

216. The potential interstate jurisdictional issues go beyond the focus of this paper.

217. FTC Staff Report, at 29-31.

218. *See generally,* New Millennium Research Council, *Not in the Public Interest – the Myth of Municipal Wi-Fi Networks: Why Municipal Schemes to Provide Wi-Fi Broadband Service with Public Funds are Ill-Advised* (Feb. 2005), http://www.newmillenniumresearch.org/archive/wifireport2305.pdf.

infrastructure, as long as Google does not share this information with the state broadband provider. Thus, municipal broadband ISP providers tiered Internet results in *de facto* network neutrality. [219]

Most notable among these states is California, where the state constitution explicitly creates a citizen's right to privacy.[220] Municipal broadband providers in California cannot monitor their user's Internet browsing, thus, *de facto* network neutrality exists. Similarly, BPL companies delivering Internet to users via state-owned or financed infrastructures cannot monitor California users. This prevents BPL companies from charging Internet application companies for bandwidth use – *de facto* network neutrality.

At this point, it is foreseeable that the electorate will compel local municipalities to offer broadband service with unfettered access to the Internet and privacy protection. An alternative solution is for the passage of national legislation that would require broadband providers to implement the precepts of network neutrality if they receive either (1) tax incentives for broadband infrastructure or (2) funds to create broadband infrastructure. This approach permits broadband companies to charge U.S. citizens and application providers, so long as their infrastructure does not receive income from the tax payers. This may thereby alleviate the significant imbalance created by using state funds to create broadband networks, which then do not provide equitable access to Application Services over the broadband infrastructure.

D. Oral Communications & Embassies in the United States

The Federal government's failure to legislate the Internet, to ensure that the Internet does not become a tiered solution and its failure to follow the precepts of network neutrality may have significant international repercussions. This is because embassies, consulates and other diplomatic missions operating in the United States must purchase ISP services from local providers both for governmental as well as personal use. In order to implement

219. *Id.*

220. CAL. CONST. art I, § 1 states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

domestic regulations and achieve network preference, these ISP providers must monitor the information transmitted to and from the embassies and consulates. This content monitoring violates the legal rights of the embassies to maintain confidential and potentially sensitive information, and consequently may compromise the national security of the countries involved in decisions made within U.S. borders.[221]

With some exceptions, foreign embassies and consulates on U.S. soil enjoy special status and are immune under U.S. law from attachment or execution.[222] However, this immunity is not absolute since these properties owned by foreign governments are not, as widely believed, an extension of the foreign state's territory, but rather, within the territory of the host nation.[223] Despite this qualified immunity, section 463 of the Restatement of Foreign Relations Law[224] states that "The premises. . .of a state's accredited

221.The authors would like to thank Kaushik Rath, Esq. for his help in developing this portion of the discussion. Mr. Rath is a member of the New York bar and practices in New York.

By way of example, if communications to and from the Indian and Pakistani Consulates in New York were monitored by ISPs, and a breach were to occur, the results could be catastrophic given their nuclear capabilities and the tension between these two nations. This example merely illustrates the potential international repercussions of a breach of data security facilitated by ISP monitoring of content and applications to and from foreign embassies and consulates. In March 2006, India and the United States announced an unprecedented agreement where the U.S. would provide nuclear power assistance to India. Elisabeth Bumiller and Somini Sengupta, *Bush and India Reach Pact That Allows Nuclear Sales*, N.Y. TIMES, Mar. 3, 2006, at A1. The agreement would require India to separate its civilian and military nuclear programs over the next eight years while the U.S. would assist India with the development of nuclear fuel to meet its escalating energy needs. Surprisingly, the agreement would also permit India to produce vast quantities of missile material, essentially allowing it to increase its nuclear weapons production up to 50 per year. If any sensitive material regarding this agreement were transmitted through the Indian Consulate in New York, hackers could breach the data security barriers placed by the ISPs and sell this information to the Pakistani government, who in turn may attempt to hinder the negotiation of the agreement. This could severely compromise both U.S. and Indian interests, and conceivably threaten global security if an ensuing conflict were to escalate.

222. 28 U.S.C. § 1609; *See also* Englewood v. Socialist People's Libyan Arab Jamahiriya, 773 F.2d 31, 34 (2d Cir., 1985).

223. *Id.*

224. RESTATEMENT (THIRD) FOREIGN RELATIONS LAW (1987), § 443. *See* also

diplomatic mission or consular post in the territory of another state are inviolable, and are immune from any exercise of jurisdiction by the receiving state that would interfere with their official use."[225] These widely adopted principles were extracted from the Vienna Convention on Diplomatic Relations on April 18, 1961 and the Vienna Convention on Consular Relations on April 24, 1963. The United States has adopted the aforementioned principles and has in fact gone further by extending key provisions of the Convention on Diplomatic Relations to the diplomatic missions of non-ratifying countries.[226]

Inviolability imposes two distinct obligations on the receiving state. The first and more commonly known duty is to refrain from taking any action within the diplomatic premise.[227] Essentially, diplomatic missions are immune from searches, seizures, attachment, execution or any other form of enforcement jurisdiction that might interfere with the premises official use.[228]

The second duty, which is more relevant to this article, imposes on the host state the duty to protect diplomatic premises from private interference. In compliance with these requirements, the District of Columbia and the U.S. Federal Government have enacted statutes curtailing permissible activity within 500 feet of diplomatic premises if the sign brings the embassy's government into "public odium" or "public disrepute."[229] The Supreme Court upheld a critical statutory provision which prohibits congregating within 500 feet of a diplomatic premise and refusing to disperse after being ordered to do so by the police.[230] Essentially, these statutes were aimed at preventing private group interference with diplomatic property.

Jonathan I Charney, Donald K. Anton and Mary Ellen O'Connell (eds). POLITICS, VALUES AND FUNCTIONS: INTERNATIONAL LAW IN THE 21ST CENTURY (The Hague: Martinus Nijhoff Publishers, 1997).

225. *Id.*

226. GUIDE TO INTERNATIONAL RELATIONS AND DIPLOMACY (Michael Graham Fry, Erik Goldstein & Richard Langhorne, eds., 2002).

227. Geoffrey Wiseman, *Pax Americana: Bumping into Diplomatic Culture* INTERNATIONAL STUDIES PERSPECTIVES 6, 409–430 (2005).

228. *See* D.C. CODE ANN. § 22-1115 (1981).

229. Boos v. Barry, 485 U.S. 312, 315 (1988).

230. *Id.* at 329-32.

The concept of inviolability elucidated by the Vienna Conventions should also apply to the manner in which private information service providers can transact with these foreign governments, specifically with regard to their capability of monitoring information transmitted to and from these diplomatic missions.[231] This monitoring is a clear example of private interference with diplomatic property, as any and all communications between diplomats and their own nation are private and confidential, and should be protected by the inviolability concept espoused by the Vienna Conventions.[232]

However, as discussed above with recent Supreme Court decisions in *Brand X* and *Verizon*, information service carriers providing broadband Internet services are not constrained by the requirements imposed on telecommunications service providers. As a consequence, the lack of a cognizable regulatory framework for these private companies can result in the infringement of the privacy rights of these foreign governments. In the absence of network neutrality, it is possible that these information service providers can monitor the content of the communications entering and exiting the walls of these diplomatic missions, thereby violating the central precepts of the Vienna Conventions. Network neutrality, however, would preclude the necessity for such monitoring by the information service providers, thereby preserving the fundamental intent of the Vienna Conventions.

VII. RECOMMENDATIONS

Even at a regulatory level (European and the United States), we have seen a shift in attitudes on the need for network neutrality (from the United States and not the case in Europe). Below are some preliminary recommendations that deal with network neutrality at an industry level without going through the legislative route.

231. *See id.*
232. *See id.*

A. Economic/Market Correct—Content Providers Compel Broadband Companies to implement Network Neutrality

Currently, one simple solution is for application providers in the United States and abroad to simply not provide their content to broadband companies, unless the companies follow the principles and contractually obligate themselves to a technological solution driven by the precepts of network neutrality. For instance, companies such as Google, Yahoo, Microsoft, and Sony could form a group and inform broadband carriers such as Comcast that their customers will not be permitted to utilize these services. The result is that Comcast consumers do not have access to the media and information services offered by these companies while those network neutral broadband companies offer such content to their consumers.

Secondly, two U.S. providers are beginning to roll out "broadband over power line" near the end of this year in Dallas by delivering high bandwidth services over power cables. [233] If more network providers do this, there would be less inclination by them to block services such as Web TV, YouTube and VoIP calls.

Thirdly, another plausible solution which the FCC should considered in the United States is the need to encourage more competition between network operators (as in Europe) so that consumers can choose to switch from one network operator to another. This could be enhanced by a network competitor offering to ease the migration process for the consumer. Furthermore, there should be more than one network operator offering to provider broadband access. If a network operator refuses to allow customers to switch providers, then FCC could investigate whether the network operator was abusing its monopoly (as in Europe).

The proposed solutions should be discussed with the U.S. telecommunications industry and the FCC to ensure that consumers' interests are a priority. This should be considered in conjunction with U.S. legislation at a Federal level to enact network neutrality legislation and ensure end-to-end connectivity.

233. Jonathan Richards, *Web TV Demands High-power Broadband* TIMESONLINE, Aug. 15, 2007, at http://technology.timesonline.co.uk/tol/news/tech_and_ web/article2265400.ece.

VIII. CONCLUSIONS

Currently, the European legal framework (in particular, the Access and Interconnection Directive) provides a robust structure to deal with access tiering between the network and application service providers, placing a greater emphasis on NRAs to impose obligations on SMP operators or, in the case of non-SMP operators, the possibility of Article 5(1) Access and Interconnection Directive to ensure end-to-end connectivity. While there may be the possibility of access tiering occurring between network and application providers, the current EU framework is sufficient to deal with this without the need for further regulations at an EU level. In short, the prevention of access tiering can be summarized by taking a thee-prong approach: EU regulation, NRAs and consumers. These three factors are likely to inhibit the types of scenarios that arise in the United States.

The current state of the U.S. law as well as the broadband debate is certain to continue for quite sometime. The U.S. Congress will need to act in order to ensure network neutrality to address the main legal concerns including,: U.S. citizens' constitutional right to privacy; the collapse of the Internet because of state-based network neutrality legislation; U.S. citizen rights to access federal or state information; and regulatory issues specific to broadband power line technology.

Two strong policy arguments further support the adoption of the network neutrality principles. The first policy argument draws from the answer to the following question: If a device performs the same technical function as a telephone, then those analogous communications should receive the same regulatory and legal protections treatment as a telephone. While the technology medium to transport the communication is new, the communication itself is unchanged. Therefore, the laws and statutes governing the oral communication themselves, not the medium, must still apply.

The second policy argument focuses on the fact that the United States prohibits both government and companies from monitoring communications in order to dictate how and with whom individuals can communicate. Specifically, failure by the government to ensure the neutrality of the network, the government is permitting broadband companies to act both as Internet service providers and

content creators, they have a financial interest in prioritizing their own content and threatening an individual's right to privacy. For example, DBG Tel Co., an imaginary national telecommunications company that acts as a service provider and phone provider via broadband technology, monitors an individual use of the Internet and intentionally degrades VoIP because they want consumers to rely solely on services provided by DBG Tel Co. To illustrate this further, it is equivalent to an analog phone provider that unbeknownst to the consumer, monitors the consumer's phone calls to prevent them from using a third party phone conference service. The analog phone company provides the conference service and refuses to let consumers use any other conference call service or charges the provider of the conference service a fee for any consumers that do use a third party conference system. Therefore, as telephone companies cannot intentionally monitor an individual consumer's communications, or control who they can call or what third-party communication services are permissible similarly, broadband companies should also not be allowed to dictate who and how individuals communicate orally online. Overall, the solution to the problem in the United States is likely to require legislation at the Federal level until the potential for a fractured Internet is foreseeable.