Revisiting Network Neutrality

Rebecca Wong

Senior Lecturer in Law
Nottingham Law School,
Burton Street,
Nottingham,
NG1 4BU,
UK

R.Wong@ntu.ac.uk

Daniel B. Garrie, JD

Editor-in-Chief,
Journal of Legal Technology Risk Management
4580 Klahanie Dr SE,
Suite 161 Issaquah,
WA 98029 USA

Daniel.Garrie@gmail.com

Daniel W. Loewenherz

P.O. Box 200701,
New Haven,
CT 06520

Daniel.Loewenherz@yale.edu

Abstract.

The paper discusses the topical subject of network neutrality, from a US and European legal perspective. The article will begin by first defining network neutrality before addressing the underpinning technology and will then compare the legal approaches adopted by Europe and the U.S. In Europe, there is an existing electronic communications regulatory framework which can be used to address the network neutrality problem which renders any further legislation unnecessary and perhaps detrimental to the current framework. In the US, however, the main concern arising is a potential for a "fragmented" Internet, which leads us to conclude that network neutrality legislation is necessary on multiple levels. The article will conclude that the US stance on network neutrality legislation will cause a seismic shift in the way we view technology and the way that networks are accessed and utilised.

Keywords: Network neutrality; Access and Interconnection Directive; network operators, Privacy

1. Introduction

While network neutrality has been the subject of heated debate in the US, the topic has received far less global attention. In this paper, the authors explore network neutrality from a European and US standpoint, with particular focus on the international implications arising from the US stance on network neutrality legislation.

The 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 US legal frameworks. The differences in network infrastructure are examined in light of the contrasting legal frameworks in the US and Europe.

2. Network Neutrality

In this paper, we use the term "network neutrality" to apply to the provision of Internet applications and services by Internet service providers (ISPs), in the context of wireless (cell-phones and PDAs) and wired communications.[1] Providers should be restricted from blocking services and software from end users.

In addition, legislative measures are unduly cumbersome upon enforcement authorities such as the FCC and other telecommunication authorities which lack sufficient network-monitoring resources.

How do regulators monitor ISPs that operate outside US borders and block applications originating from the US? Irrespective of whether this is also a European problem, networks are not confined by borders.[2]

2.1 Arguments Made for Legislation on US Network Neutrality

2.1.2. Consumer choice

The underlying rationale submitted by authors such as Wu and Lessig is that companies that restrict services deprive or degrade consumers' experiences and services. Wu argues that "blocking [services] 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."

2.1.2. Public and private property

Broadband connections are a public resource and should be used to convey data irrespective of its origination. Consumers are entitled to resources on the Internet without interference from their broadband providers.

2.1.3. Privacy of Communications[3]

Communications privacy is an important issue for end-users, particularly if they want to be able to decide whether Internet services are blocked by their ISP. Any monitoring of web pages accessible by individuals should be limited to what is necessary and in accordance with the European Data Protection Framework (European Data Protection Directive 95/46/EC and Directive on Privacy and Electronic Communications 2002/58/EC). Transparency is needed on the part of network operators if the privacy of users' web browsing activities is to be maintained.

3. E.U. Legal Framework

3.1. New Regulatory Framework for Electronic Communications

The EU regulatory framework is comprised of five main Directives.[4] 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.

The Interconnection Directive applies to networks carrying publicly available communications services, including fixed and mobile telecommunications networks. It does not apply to web-based content,[5] but rather to ISPs.

The main provision to note 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 provides 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' (emphasis added).

If an operator is found to have SMP (at wholesale level),[6] then the NRA can, under the Interconnection and Access Directive, impose the following obligations:

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

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

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.

A further point to add is that unlike in the US, the broadband market in the UK[7] is such that consumers can easily switch from one network operator to another. In the latest report[8] published by Ofcom, approximately 69% of UK Internet users surveyed thought it would be easy to switch Internet service providers. This flexibility was further reinforced by rules regarding broadband migrations between different ISPs, introduced by Ofcom on 14 February 2007[9]. All in all, it is unlikely that consumers would tolerate discrimination between service providers by their network operators.[10]

Finally, it should be added that Regulation 2887/2000[11], stipulates that access can only be refused on the basis of technical infeasibility or the need to maintain network integrity. The Regulation also requires the incumbent operators to offer shared access[12] and sub-loop unbundling.

At the time of writing, the European Commission has indicated (in its recent communication) that it will monitor legal developments of network neutrality in the US, yet whether anything will transpire on this front is still unclear. 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 need to call for the types of regulations anticipated in the US. Despite this, whether the existing regulation will be sufficient to deal with overt discrimination between broadband providers and application providers is still unclear.

3.2. UK: Communications Act 2003

The national regulatory authority in the UK, Ofcom, took the view that the existing regulatory framework does not necessitate further network neutrality regulation.

The echoes from Ofcom highlight the concerns over reasons why further regulation is not considered necessary. The current EU and UK regulatory framework already provides for remedies against SMP network operators that charge for prioritising, blocking, or degrading traffic. Ofcom acknowledges that "network neutrality rules could be developed as an iteration of the existing non-discrimination rules."

Market power is elaborated under sec. 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 by the European Commission.

Can the UK Communications Act 2003 guarantee user end-to-end connectivity? A useful example is to consider BT and Kingston, whereby its predecessor, Director of Oftel, has been able to impose obligations on BT and Kingston to provide network access on reasonable request to third parties and do so on fair and reasonable terms, conditions and charges by virtue of sec's 151(3) and 151(4) Communications Act 2003.[13]

The most recent example whereby an 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 had notified an obligation on Sky Subscriber Services Limited, the only provider of access control services for digital TV, to provide access to these services on fair, reasonable and non-discriminatory terms.

To summarise the European and UK section, the existing regulations under the Communication Act 2003 and the Access and Interconnection Directive means that that scenario of access tiering between network operators and application providers is remote. If access tiering were to occur, the NRAs have a responsibility to ensure end-to-end connectivity for non-SMP operators under Art. 5(1) of the Access and Interconnection Directive or in the case of (wholesale) SMP operators, adhere to the obligations as provided under this Directive.

4. U.S. Network Neutrality

The US debate hinges on the fear that broadband companies will support certain content based websites and not others, thereby influencing consumer actions.

If Congress does not act accordingly and mandate network neutrality through national legislation, Internet integrity will be compromised as US states are likely to enact their own legislation, which may lead to a division on the network structure (due to interstate jurisdictional clashes). This is a realistic scenario given that in June 2007,

Maine became the first state in the nation to pass laws requiring ISPs to ensure a non-discriminatory Internet.[14] Given the scope of this paper, the subject of Internet segregation will not be explored here.

Consequently, broadband providers that favour one service provider over another may violate State network neutrality legislation, privacy law (on the local, state, and national levels),[15] and specific statutes passed by States and the Federal government to provide citizens with information access.

A counter-argument to the need for regulation is that consumers will transform their buying patterns such that the broadband providers will carry the content that the consumers desire. However, should economic welfare determine whether one can call 911, read about governmental legislation, or watch political debates?

Unlike the past, national cable providers now tend to offer a full range of communications products, often bundled together. The question then is: How can a consumer migrate to a cost-effective broadband provider if such choices are limited or unavailable? And certainly, broadband carriers should block competitors who seek to deliver phone or cable services using their bandwidth. 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.

Finally, the current network neutrality debate is not considering a very costly and real potential outcome. That is, if broadband discrimination is permitted and Congress does not ensure network neutrality, the mass exodus of website national cable providers from the US to more favourable (business-wise) countries is a possibility.

4.1. Current US Framework on Network Neutrality

The Telecommunications Act of 1996 (the "1996 Act")[16], is the first major legislation addressing telecommunications since the Communications Act of 1934 (the "1934 Act") and was intended to address a new era in communications, and to serve as a framework for regulating emerging technologies and markets.

Carriers selling broadband Internet access, pursuant to recent Supreme Court decisions, are considered information services carriers. It is here that the distinction between information services carriers and telecommunication services becomes significant, since the 1996 Act regulates telecommunications carriers while information service carriers do not fall under its purview. Traditionally distinct service providers, such as cable television and telephone service providers, now find themselves in direct competition. Not surprisingly, the Courts have played a significant role in these new conflicts.

The Supreme Court's decision in *National Cable & Telecommunications Association et al v Brand X Internet Services et al*[17] (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.[18]

The FCC's ruling under the 1996 Act classified broadband cable modem service as an "information service" because Internet access was a capability for manipulating and storing information, but not a "telecommunications service," due to the integrated nature of such access and the high-speed wire used to provide it.[19] Thus, broadband cable modem service was not subject to mandatory Title II of the Communications Act of 1934, 48 Stat. 1064, as amended, 47 US.C.S. § 151 et seq., common-carrier regulation. Within weeks, the Commission then ruled that DSL was also an information service.[20] Thanks to this reclassification, DSL carriers are no longer subject to the requirement that they share DSL lines with broadband competitors; the FCC required that carriers honor existing agreements for one year, which expired in August, 2006.[21] Collectively, these decisions re-ignited the network neutrality debate.

4.2. Network Neutrality and Oral communications

The network neutrality debate focuses on whether last-mile providers are blocking access to content and applications. Network neutrality assures that telecommunication infrastructures remain "dumb," delivering content and services equally in a "best-effort." This best effort usually entails packets being delivered in a "first-in first-out" (FIFO) method at the maximum speed possible given network constraints. Under network neutrality, network operators do not decide what content users can access. Further, they cannot impede the flow or give preferential treatment to particular kinds of content.

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.[22] This market argument is erroneous because broadband

service providers (BSPs) are effectively preventing consumers from accessing an array of Internet applications and creating a tiered Internet by granting preferential treatment to application and NCPs that compensate BSPs monetarily.[23]

So far, the current debate has lacked a discussion of privacy. Within the U.S, oral communications receive protection from the legislative and judicial branches. Since *Katz v. United States*,[24] courts have routinely forbidden third parties from tapping or monitoring oral communications. However, they just as routinely permit business to track, store and sell data packets transmitted in the same way with the implied or explicit consent of either party engaged in the transmission. The digital age and VoIP[25] have muddled the jurisdictional distinction between voice and data information.[26] 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.[27]

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 in digital data packets.[28]

The courts have found telephone communications protected from governmental privacy invasions in two principal ways. [29] First, parties to a voice conversation are entitled to a "reasonable expectation of privacy" under the Supreme Court opinion of *Katz v. United States*.[30] Secondly, the Federal Wiretap Act of 1968 prevents unauthorized third-party interceptions of telephone communications, save for two scenarios: 1) the interceptor is in possession of a court-mandated order or; 2) either of the involved parties in the communication have already provided consent.[31] The *Katz* opinion explains the rationale behind the Supreme Court's oft-quoted statement that the Fourth Amendment protects people, not places,"[32] and concludes that an entity's reasonable expectation of privacy must be protected from government searches. The Federal Wiretap Act was Congress's response to the *Katz* opinion and was an attempt to prevent electronic surveillance of oral telephone communications without a court order.[33]

Title III of the 1968 Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")[34] initially afforded extensive protection to wire communications—oral communications were protected only when there were reasonable expectations of privacy[35] Because the legislation covered both face-to-face oral communications and traditional point-to-point wired communications, courts were faced with myriad interpretive difficulties.[36] To correct the problems with Title III, Congress amended the Wiretap Act by passing the Electronic Communications Privacy Act of 1986 (ECPA).[37] Congress designed the ECPA to prohibit the intentional interception of oral, wire, and electronic communications.[38] Because Congress was concerned with advancements in electronic technology that would be capable of defeating any privacy expectations, the ECPA enacted a strict set of standards for the interception of oral, wire, and electronic communications.[39] Congress further expanded the protection of wireless communication by passing the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which extended Title III to the radio portions of cellular and cordless phones.[40]

While the US courts forbid third parties to tap or monitor oral telephone communications,[41] they routinely permit data packets[42] to be tracked, stored, and sold by third parties with the implied[43] or explicit[44] consent of either party engaged in the transmission. In the digital age, however, the law-made distinction between voice and data has become unclear. 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.[45] The use of VoIP and other broadband 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.[46]

VoIP is a technology for transmitting ordinary telephone calls over the Internet. VoIP can send oral, fax and other information over the Internet, rather than through the Public Switched Telephone Network (PSTN) or regular telephone network. For example, if you are connected to the Internet, you can simultaneously exchange data, audio or video with anyone while using VoIP.[47] The convergence of separate mediums shifts the legal landscape of digital communications 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.[48]

VoIP is no longer a fledgling technology; it is rapidly becoming a mainstream communication product along with several other broadband communication technologies. Both corporate and individual consumers are using VoIP to reduce communication costs by capitalizing on their existing connections to Internet broadband infrastructure.[49]

VoIP cost savings arise[50] from the ability to transmit oral and data communications simultaneously over the same medium,[51] thereby eliminating the need for multiple phone and data lines in a home[52] or business.

While the market's invisible hand has already fostered technical innovations making some VoIP services superior to those offered by the traditional PSTN,[53] 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 to tax the transmission of data[54] and to regulate communication networks and line monopolies.[55] Second, the degree of privacy, if any, the law can provide to VoIP oral communications must be defined.[56] The taxation issue lies entirely in the hands of a legislature that is actively attempting to extend PSTN taxation to IP communications networks.

VoIP and other broadband communication technologies opens a paradigm of oral privacy, which will place a considerable strain on the existing judicial canons protecting oral and data communications. This legal privacy dichotomy poses a substantial risk that parties legitimately monitoring Internet data streams will unlawfully monitor constitutionally protected private oral communications.

Under the current legal framework, unauthorized third-party access to oral telephone communications made from the privacy of one's home constitutes an invasion of any non-consenting person's privacy. Courts will probably extend these privacy rights to VoIP communications because the Supreme Court has recognized oral communication privacy rights within the context of the home.[57] Because it is physically transmitted in the form of digital data packets over the Internet, VoIP oral communications, though essentially indistinguishable from Internet data communications, are legally protected by a constitutional right of privacy preventing third parties from tracking, tapping, storing or selling said communications.[58]

If broadband companies triumph and a tiered Internet arises, these telecommunication/broadband companies will in varying degrees monitor and intercept digital packets. This act provides the consumer with a right to bring suit against the US government, the telecommunication provider, and any other parties for violating the federal Wiretap Act and a range of State specific laws.

4.3. Oral Communications Delivered Over Municipal Broadband & Broadband Power Line Companies

Again, if the legal points above are resolved for entities that provide private broadband Internet services, the issue of State-funded municipal broadband ISPs (MISPs) remains unanswered. In this case, since the state is the broadband provider, there are greater duties lying upon the state to protect its citizens' right to privacy and provide its citizens with unfettered access to information, as set-forth under the US constitution and in some instances at the state-level. Arguably, a MISP, which does not enforce the precepts of network neutrality, regardless of whether it violates Federal and States' privacy rights, exposes itself to legal suit.

States that explicitly recognize a citizen's right to privacy (e.g. California)[59] require any MISP within that State to enforce the precepts of network neutrality. The reason for this derives from the fact that such ISPs cannot monitor a citizen's Internet usage without cause due to state laws. Since the broadband provider is incapable of monitoring a client's access, they cannot charge website providers, such as Google, as they cannot prove that said user had accessed Google via their network infrastructure. As long as Google does not share this information with the MISP, the above scenario is preserved. Thus, MISPs rend the ability to tier access impossible, resulting in *de facto* network neutrality.[60]

At this point, it is foreseeable that the electorate compels local municipalities to offer broadband service with unfettered access to the Internet and privacy protection. An alternative solution is to pass national legislation that requires broadband providers to implement the precepts of NN if they receive either (1) tax incentives for broadband infrastructure or (2) funds to create broadband infrastructure. This approach allows broadband companies to charge US citizens and service providers as long as their infrastructures do not receive taxpayer income. This thereby alleviates 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.

4.4. Oral Communications & Embassies within the United States

The US Federal government's failure to legislate the Internet to ensure that the Internet does not become a tiered solution and to follow the precepts of network neutrality may all have significant international repercussions.[61] This is because embassies, consulates and other diplomatic missions operating in the US must purchase ISP services locally both for governmental purposes as well as personal use by those residing on the diplomatic premises. In order to implement domestic regulations and achieve network preference, these ISP must monitor the information transmitted to and from these embassies and consulates. This monitoring of the content and applications by the ISPs providing broadband service to embassies in the US violates the legal rights of the embassies to maintain confidential potentially sensitive information, and consequently may compromise the national security of these countries of any and all decisions made within US borders.

Generally, foreign embassies and consulates on US soil enjoy special status and are immune under US law from attachment or execution. Despite this qualified immunity, section 463 of the Restatement states that "The premises…of a state's accredited 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."

Inviolability imposes a distinct obligation on the receiving state to protect diplomatic premises from private interference. In compliance with these requirements, the District of Columbia and the US 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."

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 regards to their capability of monitoring the information transmitted to and from these diplomatic missions.[62] This monitorization 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.[63]

However, as discussed above with recent Supreme Court decisions, 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.

5. Recommendations

Even at a regulatory level (European and the US), we have seen a divergence of views on the need for network neutrality. Below are some preliminary recommendations that deal with network neutrality at an industry level without going through the legislative route.

5.1. Market Solutions for Cable Providers Compel Broadband Companies to implement Network Neutrality

One solution is for application providers in the United States and abroad to coalesce together and decide to restrict their content from broadband companies unless the companies follow a set of principles and contractually obligate themselves to a technological solution driven by the precepts of network neutrality.

Secondly, two US providers[64] are releasing "broadband over power line" services in Dallas, Texas. If more network providers follow suit, there would be less inclination by them to block services such as Web TV, YouTube and VoIP calls.

Thirdly, another plausible solution which should be considered by the FCC in the US is the need to encourage more competition between network operators as in Europe so that consumers have a choice 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 provide

broadband access. If a network operator refuses to allow customers to switch providers, then the FCC could investigate whether the network operator was abusing its monopoly position (as in Europe).

6. Conclusion

Currently, the European legal framework (in particular, the Access and Interconnection Directive) provides a robust structure to deal with access tiering between network and application service providers. Whilst the possibility of access tiering may occur between network and application providers, the current EU framework is sufficient to deal with this without the need for further regulations.

The current state of the US law is in a state of flux and the broadband debate is certain to continue in the future. The US Congress will need to act to ensure network neutrality to address the main legal questions: US citizens' constitutional right to privacy, a fragmented Internet due to state-based network neutrality legislation, US citizens' right 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 following:

> 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 US prohibits both the government and companies from monitoring communications in order to dictate how and who individuals can communicate. Specifically, failure by the government to ensure the neutrality of these networks will allow broadband companies to act both as ISPs and as content creators. Furthermore, these companies will have a financial interest in prioritizing their own content and in threatening an individual's right to privacy. Overall, the solution to the problem in the US is likely to require legislation at the Federal level until there is foreseeable potential for a fractured Internet.

Dr 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 and Cyber law. Her main areas of specialism are in data protection and privacy. 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*, 2007, International Journal of Commercial Law and Technology, 2(1) 9-16 (reprinted in Journal of Internet Law, March 2007 and ICFAI Cyberlaw, May 2007) and "Demystifying clickstream data: a European and US perspective" in *Emory International Law Review* 20(2), 563-590 (2006).

Mr. Garrie holds a MA and BA in Computer Science from Brandeis University and a JD from Rutgers School of Law. 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 published more than 30 articles in scholarly and industry legal journals worldwide, and his writings are widely cited in legal and technology publications. Mr. Garrie is considered one of the industry's thought

leaders on topics that include consumer Web data both in the United States and abroad, digital privacy, e-discovery, VoIP, e-Discovery, SOX, digital sexual harassment, and spyware. He is frequently sought after presenter at legal and technology seminars and conferences worldwide. He can be reached via e-mail at daniel.garrie@gmail.com and archiving.

Daniel W. Loewenherz is currently a junior at Yale University, pursuing a B.A. degree in Economics and Mathematics. Following graduation from Yale in Fall 2008, he plans to matriculate into law school and pursue interests in international law. His academic interests include financial modeling, programming, and stochastic processes as applied to human behavior. He is a regular programming competitor on TopCoder.com and secured a third-place finish at the 2005 ACSL International Programming Tournament. He is currently researching the state of agricultural insurance and financial derivatives in the People's Republic of China.

[1] Zeman, Eric M. "Paper sparks wireless net neutrality debate." March 10, 2007 <http://freepress.net/news/21377>
[2] Reidenberg, Joel R. "Governing networks and rule-making in cyberspace." Emory Law Journal, 1996: 45 p. 911. Johnson, David R and David G. Post. "Law and Borders – the rise of law in Cyberspace." Stanford Law Review, 1996: 48 p. 1367. Froomkin, Michael A. "The Internet as a source of regulatory arbitrage." March 2007.
[3] "The Buzz Report; Net Neutrality: Bring it On." CNET. March 10, 2007 < http://www.cnet.com/4520-6033_1-6548559-1.html>
[4] Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, OJ L 108/33, 24 April 2002. Authorization Directive 2002/20/EC on the authorization of electronic communications networks and servicesservices OJ L 108/21, 24 April 2002. Access and Interconnection Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, OJ L108/7, 24 April 2002. Universal Service Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and servicesservices, OJ L 108/7, 24 April 2002. The Directive on Privacy and Electronic Communications 2002/58/EC concerning the protection of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37, 31 July 2002
[5]The latter half of Article 2(c) of the Framework Directive specifically provides that electronic communications services does not include 'services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.'
[6] At the retail level, Articles 17-19 of the Universal Services Directive apply.
[7] "The Communications Market: Broadband: Digital Progress Report." Ofcom. April 2, 2007 <http://www.ofcom.org.uk/research/cm/broadband_rpt-/broadband_rpt.pdf> In the UK, it was identified in the report that over a quarter (27%) of residential Internet users had changed service providers in the last quarter of 2006 (Q3, 2006).
[8] *Ibid.*, at 38.
[9] *Ibid.*
[10] Art. 5(1)(1)(a) of the Access and Interconnection Directive, which enable NRAs to impose obligations on undertakings that control access to end users to ensure end-to-end connectivity.
[11] Regulation No. 2887/2000 of December 18, 2000 on unbundled access to the local loop, O.J. 2000 L336/4. See also Ofcom. *LLU factsheet* (http://www.ofcom.org.uk/static/archive/oftel/publications/broadband/dsl_facts/LLUbackground.htm), Last accessed 7 August 2007.
[12] Shared access occurs when voice traffic and broadband access are managed by different access providers.
[13] *Review of the fixed narrowband wholesale exchange line, call origination, conveyance and transit markets*. November 28, 2003 <http://www.ofcom.org.uk/consult/condocs/narrowband_mkt_rvw/nwe/fixednarrowbandstatement.pdf> and *Review of the wholesale broadband access markets*. May 13, 2004 <http://www.ofcom.org.uk/consult/condocs/wbamp/wholesalebroadbandreview/broadbandaccessreview.pdf>.
[14] Sec. 1. 35-A MRSA § 7109. *Nondiscriminatory provision of Internet services*

[15] , M.J. Culnan, Protecting privacy online: is self-regulation working? Journal of Public Policy and Marketing 19 (1), 2000, pp. 20-26.
[16] 47 US.C.S. §§ 151 et seq.
[17] *545 US 967*
[18] 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).
[19] 540 US 398.
[20] *Ibid.*
[21] *Ibid.*
[22] Amy Schatz & Anne Marie Squeo, As Web Providers' Clout Grows, Fears Over Access Take Focus: FCC's Ruling Fuels Debate Between Broadband Firms and Producers of Content, WALL ST. J., Aug. 8, 2005, at A1
[23]Tripp Blatz, Three Carriers Have Now Blocked Access to Ports for VoIP, Vonage Chairman Alleges, TELECOMM. MONITOR, Aug. 23, 2005.
[24] 389 US 347 (1967)
[25] Daniel B. Garrie, Matthew J. Armstrong, Donald P. Harris, Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?, 29 Seattle U. L. Rev. 97 (2005).
[26] *Ibid*
[27] Daniel B. Garrie, Matthew J. Armstrong, Donald P. Harris, Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?, 29 Seattle Univ. L. Rev. 97 (2005).
[28] *Ibid.*
[29] Frierson v. Goetz, 227 F. Supp. 2d 889, 896-97 (M.D. Tenn. 2002) (describing a two-part test for determining qualified immunity).
[30] 389 US 347, 350 (1967).
[31] 18 US.C. §§ 2510-2521 (2004).
[32] Katz, 389 US at 351.
[33] United States v. Andonian, 735 F. Supp. 1469, 1471 (C.D. Cal. 1990); S. REP. NO. 90-1097, at 66-72 (1968); 1968 US Code & Admin. News 2110, 2153-2159.
[34] Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 212 (1968).
[35] United States v. McKinnon, 985 F.2d 525, 527 (11th Cir. 1993)
[36] Edwards v. Bardwell, 632 F. Supp. 584, 589 (M.D. La.), aff'd, 808 F.2d 54 (5th Cir. 1986)
[37] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 US.C. §§ 2510-2521, 2701-S2710, 3117, 3121-3126 (1986)).
[38] S. REP. NO. 99-541 (1986), reprinted in 1986 US.C.C.A.N. 3555, 3555-3557.
[39] 18 US.C. § 2518 (2004).
[40] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (amending 18 US.C. § 2510 (2004)).
[41] Katz v. United States, 389 US 347, 353 (1967)
[42] Vonage Holdings Corp. v. Minnesota Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 994 (D. Minn. 2003)
[43] In re DoubleClick, Inc. Privacy Litig.
[44] In re Pharmatrak, Inc., 329 F.3d 9, 19-22 (2003); Directv, Inc. v. Spokish, 2004 WL 741369, at *3, 17 (M.D.Fla. Feb 19, 2004); Dyer v. Northwest Airlines Corporations, 334 F. Supp. 2d 1196, 1198 (D.N.D. Sep 08, 2004); Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 643 (E.D.Va. Jul 12, 2004).
[45] *Vonage*, 290 F. Supp. 2d at 1000-03.
[46] FROST & SULLIVAN, VOIP EQUIPMENT 2003 WORLD MARKET UPDATE (2003)
[47] CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1999).
[48] Compare Katz v. United States, 389 US 347, 353 (1967)
[49] Stan Gibson, *VoIP Passes Nissan Road Test*, EWEEK, Jan. 24, 2005, at 33.
[50] Paul Taylor & Peter Thal Larsen, *Time Warner Cable Plans Big Push Into Internet-Based Phone Services*, FIN. TIMES, Dec. 9, 2003, at A1.

[51] Internet Engineering Steering Group, Internet Architecture Board, *IETF Policy on Wiretapping*, RFC 2804, INTERNET ENG'G TASK FORCE (May 2000) (discussing how VoIP uses the Internet's open network architecture and stating that VoIP and Internet communications transmit on a single interconnected digital network).
[52] By the end of 2006, more than half of all 110 million-odd households in the US 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. Peter Grant, *Here Comes Cable..*, WALL ST. J. Sept. 13, 2004 at R4.
[53] Sheff, David, *Betting on Bandwidth*, WIRED, Feb. 2001, at 144-56.
[54] Congress's decisions to tax and regulate VoIP technology are beyond the scope of this paper.
[55] Declan McCullagh, *Congress Proposes Tax on All Net, Data Connections*, Jan. 28, 2005, *available at* http://news.com.com/Congress+proposes+tax+on+all+Net,+data+connections/2100-1028_3-5555385.html (last visited July 20, 2005).
[56] Katz v. United States, 389 US 347, 353 (1967)
[57] United States v. Karo, 710 F.2d 1433, 1441 (10th Cir.1983)
[58] Bartnicki v. Voppe, 532 US 514 (2001)
[59] FTC Staff Report, at 29-31.
[60] 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
[61] Contribution by Kaushik Rath.
[62] Boos v. Barry, 485 US 312 (1988)
[63] *Id*.
[64] Richards, Jonathan. *Web TV demands high-power broadband*. August 15, 2007 <http://technology.timesonline.co.uk/tol/news/tech_and_web/article2265400.ece>.