UC Irvine

UC Irvine Previously Published Works

Title

User and ISP Rights of Device Attachment and Device Management

Permalink

<https://escholarship.org/uc/item/90j7x704>

Journal

ACM Transactions on Internet Technology, 13(2)

ISSN

15335399

Authors

Jordan, Scott
Shaffer, Gwen

Publication Date

2013-12-01

DOI

10.1145/2513227

Peer reviewed

User and ISP Rights of Device Attachment and Device Management

SCOTT JORDAN, University of California, Irvine
 GWEN SHAFFER, California State University, Long Beach

Internet research often assumes users may connect devices without consent by their service providers. However, in many networks the service provider only allows use of devices obtained directly from the provider. We review how United States communications law addresses the rights of users to connect devices of their choice. We explicate a set of user and service provider rights. We propose legal requirements for attachment and management of devices. We illustrate how these proposed regulations would affect the services currently offered on telephone, cable, satellite, video networks, and cellular networks, as well as on the Internet.

Categories and Subject Descriptors: C.2.3 [Computer-Communication Networks]: Network Operations; K.4.1 [Computers and Society]: Public Policy Issues; K.5.2 [Legal Aspects of Computing]: Governmental Issues

General Terms: Economics, Legal Aspects, Management

ACM Reference Format:

Jordan, S. and Shaffer, G. 2013. User and ISP rights of device attachment and device management. *ACM Trans. Internet Technol.* 13, 2, Article 6 (December 2013), 20 pages.
 DOI: <http://dx.doi.org/10.1145/2513227>

1. INTRODUCTION

The Internet is steadily progressing toward supporting a wide variety of heterogeneous devices. Whereas once a residential connection to the Internet was comprised of only a cable or DSL modem attaching one computer, it is now common that a residential network comprises a cable or DSL modem, a wireless router, computers, printers, network-attached storage, wireless adapters, and set-top boxes. A significant number of residential networks also directly connect televisions, music systems, VoIP phones, and home gateways. Cell phone networks now connect to the Internet smartphones, tablets, e-readers, and navigation devices. A wider variety of Internet-connected devices is expected, and the Internet of Things is the subject of many papers.

Networking researchers often assume that users should be able to connect devices without requiring prior permission of an Internet Service Provider (ISP). The vision inherent in such an Internet of Things is usually that of an open network, in which a user has the ability to connect devices of their choice to the network. In the early broadband era, ISPs often prohibited in a residential user's terms of service, the connection

This work has been supported by the National Science Foundation.

Portions of this work appear in Jordan and Shaffer [2012]. Portions of this work also appear in Jordan and Shaffer [2011], which is directed at the policy community and focuses on development of statutory language; this article is directed at the networking community and focuses on the relationship of policy to network architecture.

Authors' addresses: S. Jordan, Department of Computer Science, University of California, Irvine; email: sjordan@uci.edu; G. Shaffer, Department of Journalism and Mass Communication, California State University, Long Beach.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.

© 2013 ACM 1533-5399/2013/12-ART6 \$15.00

DOI: <http://dx.doi.org/10.1145/2513227>

of any device other than a single computer. Today, however, a residential broadband subscriber would view such a restriction as ludicrous.

With such an open network vision, networking research on an Internet of Things is almost always focused on creating standardized interfaces and protocols. The goal of standardization is to support interconnection and interoperability of devices, thus creating the platform that enables heterogeneous devices. The preference in networking has generally (but not always) been toward standards rather than proprietary methods. Such open approaches have usually dominated in the networking marketplace due to a strong network effect, in which the value of connecting to the Internet is dominated by the utility a user obtains through being able to communicate with other people and devices.

In addition, networking researchers usually assume that users and their ISPs will share control of the devices a user places in a residential network or attaches to the Internet. The decision of whether a user or the ISP controls each device and protocol is usually assumed to be made on the basis of efficiency and effectiveness.

However, these three assumptions by networking researchers—user ability to connect devices of their choice, standardized protocols, and shared control based on effectiveness—are violated by many devices offered by or mandated by ISPs. We briefly discuss three such devices: residential gateways, set-top boxes, and smart phones.

Residential connection to the Internet is increasingly provided through a residential gateway supplied by an ISP, which allows connection of a wide variety of devices through the gateway. However, an ISP sometimes mandates use of a residential gateway it provides, precluding the user from attaching a router or gateway of their choice. In addition, the ISP maintains control over nearly all protocols used in the gateway, depriving users of the use and control of certain protocols that the gateway may block.

Cable and satellite television is increasingly accessed through a set-top box leased by the provider to the subscriber. In some cases, the consumer has no other option, whereas in other cases the consumer may elect to purchase a set-top box offered by a consumer electronics company but will often find that it does not provide access to all video content. The set-top box supplied by the video provider often limits the devices that a consumer may connect to the network and thereby limits access to video content. The set-top box may also use proprietary protocols to access certain information streams, and thereby eliminate the ability of other user-chosen devices to provide functionality such as video navigation. These impediments all challenge the open network model assumed by most networking researchers.

Smart phones used on cellular networks are an even greater challenge to open networks. A cellular provider often exercises control over the devices used on its network through a combination of terms of service and device pricing. The provider often reserves the right to control nearly all communication protocols on the device. It is not uncommon for providers to lock devices to their own networks, or to cripple functionality of devices.

Such restrictions impede the development of a competitive heterogeneous market for devices, and thus impede the likelihood that networking research on this topic will lead to innovative new devices. The ability of an ISP, video provider, or cellular provider to limit the devices attached to their networks, to use proprietary protocols, and to maintain control over protocols sent through their networks, is determined by communications law. However, the law in almost all countries has been written separately for different communications technologies.

In the United States, users' ability to attach devices of their choice to the telephone network is guaranteed by regulation, providing that the device does not harm the network. Users' ability to attach set-top boxes of their choice on a cable television network is guaranteed by law, but not on a satellite television network. Users have no legal

right to use devices of their choice on cellular networks. The Federal Communications Commission (FCC) has only very recently created a regulation that gives users the right to use non-harmful devices of their choice on fixed Internet broadband.

This fragmented approach to regulation of consumer device attachment is doomed to failure as the Internet becomes the dominant network supporting communication and supporting access to electronic content. Thus, a great need exists to create a unified legal framework that can dictate a user's right to attach devices to the future Internet.

Academic literature offers minimal guidance on how to construct such a legal framework. Wu [2007] focused on whether cellular subscribers should be able to attach wireless devices of their choice, and argued for the extension of current rules that give such rights to users of telephone networks, to cellular networks. He proposes that industry or the FCC should define a basic air interface for wireless devices, and that this basic air interface be used to prohibit cellular carriers from banning attachment of any compatible non-harmful device. He also proposes that there be a prohibition on locking of devices to a carrier. In response, Hahn and Litan [2007] argue that there is sufficient wireless competition to avoid market failure and that innovation in wireless devices and applications is thriving. They claim that the results of an economic analysis show that the benefits of device subsidies, device exclusivity, and limits on devices, and on applications, outweigh the costs of each. There is no similar academic literature addressing device attachment in converged networks. A number of papers have argued that communications law must be rewritten to apply to converged networks (see e.g. Bar and Sandvig [2000], Werbach [2002], Whitt [2004]), but none have directly addressed how this could be accomplished with respect to device attachment.

In this article, we propose a legal framework for attaching devices to the Internet. The framework ensures users the right to connect devices of their choice while simultaneously ensuring network providers the right to reasonably manage their networks. It is consistent with current user and provider rights in the United States on telephone networks, and strengthens user rights on cable, satellite, and cellular networks. It can be gracefully applied to residential networks attached through cable and DSL modems or through residential gateways, and it addresses which protocols and devices should be controlled by users and which by providers. It does not require separate rules for telephone, cable television, satellite television, and cellular networks, or for the Internet.

Although we believe that the current legal and regulatory approach cannot survive technology convergence, this article does not address whether the proposed legal framework is the best one to address device attachment in converged networks. First, economic analyses are required to determine the economic advantages and disadvantages of various legal approaches. Second, legislative and regulatory bodies must attempt to identify the most socially beneficial approach for their country. Such evaluations may agree or disagree with an approach dominantly based on network architecture, since they will take into account economic and public policy concerns.

We thus intend the contribution of this article to be twofold: (1) to educate network researchers about issues of device attachment under current law, and (2) to illustrate a potential legal framework for device attachment in a converged network if legislative and/or regulatory bodies are looking for a relatively open approach. Since we are unaware of any other proposals for potential legal frameworks that address converged networks, we consider the proposal here as an existence proof that a unified framework can be constructed.

The problems addressed in the article are present in many countries. The legal issues regarding conflicting laws addressing cable networks, mobile networks, telephone networks, and broadband Internet access are present in many countries, although the specific laws differ country by country. However, the technical issues regarding

device attachment, device control, and traffic management, are international. We believe that the proposed rights and limits concerning device attachment, device control, traffic management, and service plan integration, could be successfully applied internationally, because they rely on concepts emanating from network architecture which is itself international. When the article progresses to establishing each of these concepts in statutory language, its focus narrows to the United States, since statutory language is highly dependent on existing law.

In Section 2, we analyze both the technologies and legal models for device attachment to telephone networks, the Internet, video networks, and cellular networks. In Section 3, we present a set of rights that users should have, and a set of rights that providers should have, and define the scope of the application of these rights. In Section 4, we consider where and how a service provider's network connects to a user network or user device, and propose legal requirements for attachment of devices to provider networks. In Section 5, we consider management of devices, and propose limited rights of service providers to control specific elements of user devices. In Section 6, we consider traffic management, and propose limitations on integration of devices with service plans, a definition of reasonable traffic management, and a transparency principle. In Section 7, we briefly address a communication provider's right to forbearance from regulations unnecessary to ensure user rights. Finally, in Section 8, we revisit the technologies and regulatory models from Section 2 and discuss how our proposed legal framework would affect the services offered by each.

2. CURRENT TECHNOLOGIES AND REGULATORY MODELS

In this section, we discuss the current technologies for device attachment to various networks and the legal models in the United States that are used to regulate device attachment. We will discover that the legal models are inconsistent with one other. Although they cannot be directly applied to converged networks, they contain elements that will be useful in constructing a unified legal framework.

2.1. Telephone Networks

Prior to 1968, telephone companies in the United States could block users from attaching any device to the telephone network other than devices they supplied. Telephones were usually directly connected by wire. In 1968, the FCC decreed that telephone companies must allow users to attach devices, providing that the devices do not harm the network [FCC 1968]. The FCC developed regulations in 1975 to detail the requirements for device attachment to telephone networks. These regulations, which appear in Title 47 Part 68 of the Code of Federal Regulations [FCC 1975], referred to as *Part 68 rules*, first define a demarcation point as the geographical point at which the telephone companies' network interconnects with the customer premises wiring. The telephone company is responsible for the wiring on its side of the demarcation point, and the subscriber is responsible for wiring on the residential side of the demarcation point. The telephone company may interconnect with customer premises wiring either via wire or via standardized jack. Today, the demarcation point usually consists of a RJ11 jack within the User Network Interface box, where the wiring enters a residence. A subscriber of telephone service has the right to use devices (called customer premises equipment or terminal equipment) provided that the devices do not cause harm to the telephone network. Harm is defined in terms of electrical hazards, damage to telephone company billing equipment, or degradation of service to other telephone network users. A user has two options for ensuring that no harm is caused. The first option is to purchase devices that are certified not to cause harm; certification is provided by an independent body. The second option is to insert

protective circuitry between the device and the demarcation point; the protective circuitry must be certified to protect the telephone network.

Users of telephone networks thus have strong legal protection to attach devices of their choice to telephone networks. This right has resulted in a competitive market for telephones, and in the development of other devices such as answering machines and modems.

2.2. Broadband Internet Access

Residential broadband Internet access in the United States is most often provided via either DSL modem or cable modem.

DSL modems are essentially an attachment to the telephone network. Broadband Internet access via a DSL modem is provided by branching out either at the User Network Interface or somewhere within the customer premises wiring. All wiring and devices on the customer's side of the telephone network demarcation point are the choice of the user. DSL modems are certified not to cause harm to the provider's network, primarily by certifying that they follow standard protocols such as ADSL. However, unlike voice telephone network devices, the ISP controls a portion of the DSL modem. Access to the particular broadband Internet service purchased by the subscriber is often implemented by the ISP controlling parameters within the DSL modem. For instance, the ISP may limit the maximum upload transmission rate to a rate specified by the user's subscribed plan. More specifically, we find that the ISP controls the operation of layers 1 through 3 of the ISP's interface of the DSL modem. In addition, the ISP controls certain elements of layers 4 through 7 of the ISP's interface of the DSL modem, e.g. blocking of NetBIOS traffic from the user's residential network to the ISP's network, control over DHCP, and operation of SNMP. However, the user controls all layers of the interface of the DSL modem facing the user's residential network.

Cable modems are an attachment to a cable television network, not to the telephone network. However, the technology is similar. There is typically a junction box at the entry to the customer premises or at the curb. The junction box usually contains either a coaxial cable junction or an optical to coaxial adapter. Although not legally a demarcation point, this junction box serves a similar role in that all wiring and devices on the customer's side of the telephone network demarcation point are the choice of the user. Although there is no Part 68 requirement to ensure devices do not harm the network, harm is prevented through use of certified standards such as DOCSIS. The ISP controls the operation of layers 1 through 3 and certain elements of layers 4 through 7 of the ISP's interface of the cable modem, while the user controls all layers of the interface of the DSL modem facing the user's residential network.

More recently, some broadband Internet access providers require the use of a residential gateway to access certain services. Verizon requires the use of a residential gateway for its FIOS Internet service. Verizon usually places an optical jack followed by a POTS splitter in the User Network Interface near the demarcation point, and feeds the Internet service into the residence via a PPPoE network. The residential gateway is required to translate PPPoE to either Ethernet or Wi-Fi. Verizon provides a residential gateway but does not require its use, and thus some users have replaced it with a residential gateway of their choice. As with DSL modems, the subscriber may use devices of their choice on the side of the residential gateway facing the user's residential network. Harm to Verizon's network is prevented through certification that the residential gateway implements the PPPoE standard. Verizon governs access to services via control of layers 1 through 3 of the residential gateway, e.g. through control over PPPoE, and also controls certain elements of layers 4 through 7 of the ISP's interface of the residential gateway in order to perform network management.

AT&T similarly requires the use of a residential gateway for its U-Verse Internet service. AT&T usually places an RJ11 jack in the User Network Interface near the demarcation point, and feeds the Internet service into the residence via twisted pair. AT&T requires the subscriber to use a residential gateway it provides. The proprietary residential gateway routes Internet traffic onto an Ethernet and/or Wi-Fi network. The subscriber may use devices of their choice on the side of the residential gateway facing the user's residential network, but may not replace the residential gateway. AT&T governs access to services and implements network management via control of the majority of all layers of both sides of the residential gateway. Since the gateway also implements DHCP and NAT for the residential network, and contains a firewall, users have no alternative implementation of these protocols.

Until recently, users had no legal right to attach devices to broadband Internet access networks. The Telecommunications Act of 1996 [U.S. Congress 1996] created two categories of services over telephone networks. *Telecommunication services* are defined 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." *Information services* are defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." The Telecommunications Act of 1996 placed telecommunications services, but not information services, under Title II of the Communications Act. As a result, Part 68 regulations apply only to telecommunication services, not to information services. In 2002, the FCC ruled that cable modem service is an information service, not a composite of telecommunications service and information service [FCC 2002]. In 2005, the FCC similarly ruled that DSL modem service is an information service, not a composite of telecommunications service and information service [FCC 2005a]. Both rulings are controversial, and we will disagree with them below.

As a consequence of these classifications, the FCC removed any user rights to attach devices of their choice to broadband Internet access via either cable modems or DSL modems. Thus ISPs using either technology had the legal right to restrict user devices.¹ As discussed in the preceding, in the early days of such service, some ISPs restricted use to a single computer attached to the cable or DSL modem. Today, such limitations are rare, but AT&T does not allow a subscriber to connect a residential gateway of their choice even if it is certified not to harm AT&T's network.

In December 2010, the FCC issued the Open Internet Order [FCC 2010b]. This order—mostly focused on issues of net neutrality—prohibits fixed broadband Internet access service providers from blocking non-harmful devices unless such blocking is deemed reasonable network management. It also requires fixed broadband Internet access service providers to publish any restrictions on the types of devices and any approval procedures for devices to connect to the network. However, the FCC has yet to define *harm*, or to address user versus ISP control over devices, subsidization of devices, and distribution of content to devices. It is not yet clear whether the new rules would interpret AT&T's requirement to use its residential gateway as legal or illegal.

2.3. Video Service

Multichannel video service in the United States is most often provided via either cable television networks or satellite television service.

Cable television service is usually obtained from a junction box at the entry to the customer premises or at the curb. The junction box usually contains either a coaxial

¹The FCC did, however, continue to debate user rights, see e.g. the FCC's 2005 set of principles [FCC 2005b].

cable junction or an optical to coaxial adapter. Video service is usually sent via coaxial cables and splitters through the residence to a set-top box. Users may attach devices via the set-top box.

Prior to 2007, cable television providers could require the use of a set-top box they supplied. However, the Telecommunications Act of 1996 required the FCC to assure the commercial availability of equipment used by consumers to access multichannel video programming and other services from vendors not affiliated with the cable television provider. Starting in 2007, the FCC required cable television providers to allow subscribers to obtain set-top boxes from unaffiliated vendors, providing that the set-top box supports the CableCARD standard. The cable television provider must supply a PCMCIA CableCARD to insert into the set-top box, and the CardCARD governs access to services, e.g. channels. Although there is no Part 68 requirement to ensure devices do not harm the network, harm is prevented through use of certified standards such as DOCSIS.

Satellite television is usually provided via a satellite dish to a set-top box. There is commonly a coaxial junction in between the satellite dish and the customer premises, with coaxial cables continuing into the set-top box. Users may attach devices of their choice via the set-top box. Unlike cable television providers, satellite television providers are not required to allow subscribers to obtain set-top boxes from unaffiliated vendors. Thus, the set-top box is usually provided by the satellite television provider, and the user must use this box. The set-top box often allows an access card to be inserted which governs access to services. However, this access card usually does not follow the CableCARD standard, and thus subscribers can often not replace the set-top box with one of their choice.

Although the CableCARD requirement gives users the right to attach devices of their choice, it has largely failed to encourage a competitive market for set-top boxes. According to the FCC, part of the reason is that CableCARDS did not allow access to two way services such as video on demand, and they required users to upgrade set-top boxes often to keep up with advances in the cable television providers services. In response, the FCC is considering replacing CableCARD with a new regulatory model dubbed AllVid [FCC 2010c]. The AllVid approach would allow a cable television provider to require the use of a proprietary adapter capable of performing only limited functions. These functions would include serving as a modem, governing access to services, content protection, and routing. However, an adapter would not be allowed to include navigation functions including programming guides and search functionality. The adapter would either be a small device that attaches to another device or a gateway that attaches to other devices via an open standard such as Ethernet. Users would have the right to attach devices of their choice on the residential network side of the adapter.

2.4. Cellular Networks

Cellular telephone providers exercise a great deal of control over the devices used on their networks. Specifically, they control availability, subsidization, and functionality of devices, as well as the ability to lock them.

Each provider uses standardized air interface protocols, e.g. GSM or CDMA. One could argue that the air interface protocol essentially serves as a User Network Interface and thus as a demarcation point, since it separates the cellular provider's network from the device and user. Despite this, many providers claim that the device is part of their network. Certification that devices properly implement standardized air interface protocols ensures that devices do not harm the network. Devices can be used on the network of a subscriber's chosen cellular provider, and also on the networks of other cellular providers using the same air interface protocol if roaming is allowed.

All providers offer devices directly to their subscribers. Providers differ as to whether they allow a subscriber to use any device of their choice on the provider's network; some providers, e.g. AT&T, only allow devices obtained through the provider. Cellular providers often require exclusive contracts from the manufacturers of devices, so that the provider can advertise that consumers can only obtain certain popular devices in conjunction with their own service. Thus a consumer may not be able to choose a particular device even if it is compatible with their desired cellular provider's air interface.

Regardless of whether cellular providers allow subscribers to use devices obtained from other vendors, providers almost universally subsidize devices they offer directly to subscribers. In return for this subsidy, they require a minimum service contract duration and use termination fees to enforce the contract. The subsidy may approximately reflect the revenue stream earned during the contract period, but it may be more substantially based on the popularity of the device. Termination fees may approximately reflect the subsidy, but often they do not decrease over the duration of the service contract. Many providers lock subsidized devices, and thereby limit device use on competing cellular providers' networks; sometimes the locking may continue even after the service contract duration is satisfied.

A subscriber's access to services is governed by the cellular provider, either through signaling from the provider's network or using information stored on a SIM card. However, many cellular providers limit the functionality of the device. Sometimes this is done by crippling functionality that the device manufacturer implemented on the device. Sometimes this is done by limiting the applications that a subscriber may run on their device.

Current law in the United States places few mandates on cellular providers with respect to device interconnection. There is no Part 68 requirement that providers allow subscribers to interconnect devices of their choice. Cellular providers are required to allow roaming of voice service on any technologically compatible network at reasonable and not unreasonably discriminatory terms and conditions. Because they are not required to support roaming of data services, many do not. The recent Open Internet regulations prohibit fixed broadband Internet access service providers from blocking non-harmful devices but do not extend this prohibition to mobile Internet access service providers. The regulations also prohibit fixed broadband Internet access service providers from blocking applications. By contrast, mobile Internet access service providers are prohibited only from blocking applications that compete with the provider's voice or video telephone services unless such blocking is deemed reasonable network management. Cellular providers can thus legally restrict devices and some applications used on their networks, providing that they disclose any third-party device and application certification procedures.²

3. A UNIFIED LEGAL FRAMEWORK FOR DEVICE INTERCONNECTION

In the previous section, we saw different regulations apply to device interconnection in telephone networks, Internet, multichannel video networks, and cellular networks. In this and the following sections, we present our proposal for a legal framework that can be applied to all of these types of networks.

Legal frameworks can be constructed in many manners. Sometimes construction starts with an economic analysis that identifies when and where market forces do not produce socially optimal results; a legal framework can be targeted to address such market failures. However, sometimes construction starts with existing legal principles;

²However, cellular providers using a particular block of spectrum cannot deny, limit, or restrict the ability of their customers to use the devices and applications of their choice on this spectrum, see FCC [2007].

a legal framework can attempt to apply these principles to an evolving world. In this article we adopt the latter approach. We first present as goals a set of user rights and a set of provider rights that are derived from existing legal principles. We then define the scope of the application of these rights. In the following sections, we formulate a legal framework that can be used to provide these rights.

3.1. User and Provider Rights

We believe that a legal framework should be constructed to attempt to ensure a set of rights both to subscribers of communication services and to providers of communication services. We believe a balanced approach that provides rights to both stakeholder groups will maximize social welfare. Communications law has a long history of supporting such rights.

We start with the following rights that users should have.

U1. Users of communications services are entitled to connect any legal device to a communications network, so long as that device does not cause harm to the network.

U2. Users of communications services are entitled to run applications of their choice on their devices.

U3. Users of communications services are entitled to choose a communications provider in a competitive market place.

U4. Users of communications services are entitled to transparency in terms of billing, traffic management, device restrictions and all other aspects of their communications services.

In 2005, in the early days of the net neutrality debate, the FCC issued a set of principles [FCC 2005b] that it proposed should apply to consumers and providers of telecommunications for Internet access. Right U1 is modeled on the FCC's proposed right of consumers to connect their choice of legal devices that do not harm the network. Right U2 is modeled on the FCC's proposed right of consumers to run applications and use services of their choice. Right U3 is modeled on the FCC's proposed right of consumers to competition among network, application, service, and content providers, but we omit the reference to application, service, and content providers since that is outside the scope of this article. Right U4 is modeled on transparency principles later proposed by the FCC and many stakeholders.

We continue with rights that communication providers should have.

P1. Communication providers are entitled to charge for communications services provided to their subscribers.

P2. Communication providers are entitled to the use of reasonable network management.

P3. Communication providers are entitled to forbearance from regulations when they are not necessary to ensure user rights.

Right P1 is original; it is intended to make it clear that user rights are limited by the communications services they have purchased from their communication provider. Right P2 is modeled on FCC's proposed net neutrality rules [FCC 2009], which makes all user rights subject to reasonable network management; rather than incorporating reasonable network management into each user right we find it more straightforward to list it as a communication provider right. Right P3 reflects a provision of communications law that specifies the conditions under which any communications regulation should be exempted; exemptions are generally granted when a marketplace is viewed as sufficiently competitive.

These rights should not be construed as absolute. They must be considered in relation to each other and to other provisions of law and regulation.

3.2. Communication Services

Before constructing a legal framework, we must define the scope of its applicability. The relevant current federal communications law in the United States is contained in the Communications Act of 1934, as updated by various laws passed since its original introduction. It was separately developed for telephone, cable video, and cellular networks. Only recently has communications law begun to address the Internet.

Title II of the Communications Act contains laws pertaining to telephone networks. It prohibits providers of public telephone service (dubbed *common carriers*) from unreasonable discrimination in charges or practices of communications services by any means or device. It also regulates interconnection with other telecommunication carriers, in particular requiring incumbent local exchange carriers to interconnect with other carriers on rates, terms, and conditions that are just, reasonable, and nondiscriminatory. Providers of cellular telephone service are subject to a portion of Title II, including the prohibition on unreasonable discrimination.

Title VI contains laws pertaining to cable networks. It does not contain similar prohibitions on unreasonable discrimination and it does not require interconnection, but it does prohibit unfair methods of competition or unfair acts or practices, and certain types of discrimination in prices, terms, and conditions of sale.

There is no similar body of communications law in the United States that directly addresses the Internet. Title I provisions are applicable to all communications activities, including those not covered by other titles. The FCC in part used these general provisions to justify its Open Internet regulations. In addition, Title I includes a provision instructing the FCC to forbear from applying regulations unless they are in the public interest and required to ensure just and reasonable practices.

Our goal is to create a unified legal framework that addresses connection of user devices. We wish to include telephone networks, cable and satellite television networks, cellular networks, and the Internet.

A number of papers have suggested using layers as a tool to formulate communications policy. Lessig [2001] considers a model consisting of physical, logical, application, and content layers. He argues that the physical and logical layers of the Internet have historically been neutral. He believes it is acceptable for the physical layer to be closed, but proposes that the logical layer should be open and act as a commons. Werbach [2002] uses a similar set of four layers: the physical layer corresponds to OSI layer 1, the logical layer to OSI layers 2–6, and the application and content layers share OSI layer 7. He argues that communications policy should be formulated around these layers, with open interfaces between them. Solum and Chung [2003] propose a six layer model, and argue that communications policy should attempt to respect the integrity of layers and to place regulation at or near the layer where the problem occurs. Whitt [2004] suggests a four layer model similar to Werbach's, and presents principles concerning how layers should inform policy formulation.

Although neither the U.S. Congress nor the FCC have yet adopted layers in the crucial regulatory definitions, we see great value in this approach. The layered approach allows unification of treatment for all the types of networks we wish to consider. However, we believe the relevant distinction is between functionality that must be provided within the access network and functionality that can be provided elsewhere in the Internet. As a starting point for this delineation, consider redefining information services as functions placed above the network layer and defining communication services (to replace telecommunication services) as functions placed at or below the network layer, and applying these two terms to all types of networks. As a consequence, functions that must be implemented at each IP hop would be classified as telecommunication services. This approach is generally consistent with current definitions of telecommunication services and information services. Specifically, protocols at or below the

network layer are concerned with transmission and routing, while protocols above the network layer are concerned with generation, acquisition, storage, and processing of information.

However, a purely layer-based delineation of infrastructure and applications is insufficient. It fails to capture the principle that communication services containing functionality must be provided within the access network. While the network layer and below contain most of such protocols, e.g. routing, addressing, and QoS, some protocols must be provided within the access network but not at every IP hop, e.g. DHCP.

For the purposes of this policy issue, we propose that communications services be defined precisely and legally by the following.

Communications Services. The term *Communications Services* means all services; (a) over a network that uses a public right-of-way; and (b) that reside at or below the network layer or are required to manage the network.

Maintaining a distinction between communications services and information services is critical to formulation of good communications policy. Communications services can only be provided by carriers, and must be provided by each carrier within their autonomous system. Such services include multiuser sharing of a wire or frequency (e.g., Ethernet or WiFi), routing (e.g., IP), and address assignment (e.g., DHCP). Communications services require large investments in loops or wireless spectrum and switches or routers. These large initial fixed costs of the business are high relative to the costs per incremental customer served, and thus such communications services have a natural economy of scale that serves as a high barrier-to-entry. This high barrier-to-entry leads few carriers to offer service in any particular geographical region. The proposed delineation also helps with correct application of the end-to-end principle. Using the new terminology, we can view the principle as a suggestion that network functionality should be implemented in communication services (at every IP hop) only if it cannot be implemented effectively in information services (often solely at the endpoints).

In contrast, information services can be provided by carriers or by many other application providers on the Internet and can be placed at many locations within the Internet. Such services include email, Web hosting, caching, voicemail, and the portions of VoIP and IPTv that can be offered by independent application providers. Internet application services usually have fixed costs that are small relative to incremental costs, and thus there is usually a low barrier-to-entry, which leads to a competitive market with a large number of application providers. We recognize that some protocols that have usually been implemented in the access network (e.g., DNS, POP, and SMTP) are thus classified as information services. We believe this is appropriate, since these functions could be offered by an application provider other than the access carrier.³

Further discussion of this proposed delineation between communication and information services can be found in Jordan [2009].

4. DEVICE ATTACHMENT

We start by considering where and how a service provider's network connects to a user network or user device. The architectural and legal details of this interconnection can greatly impact users' abilities to attach devices of their choice.

³We note, however, that our proposed definition of communication services differs from the current definitions of telecommunications service not only by the use of layering, but also by its application to all networks that use a public right-of-way, as opposed to the offering of telecommunications for a fee directly to the public. We believe that use of a public right-of-way is the correct rationale for regulation, and that a restriction to services offered for a fee directly to the public will cause increasing difficulty as it becomes increasingly difficult to distinguish offerings to consumers and to application providers. However, further study of the implications is clearly warranted.

In the telephone network, there is a legally mandated *demarcation point* that defines the place and method of interconnection. ISPs and cable television networks usually connect to a user's network at a similar junction box. However, providers are not legally required to do so, and often own some user devices such as residential gateways and set-top boxes. Satellite television and cellular providers connect via an air interface at a satellite dish or wireless device. However, cellular providers occasionally claim that user devices are part of the service provider's network.

In order to ensure a user's rights to connect devices (U1), we must first define where the service provider's network ends and the user's network begins. In telephone networks, Part 68 regulations define a *demarcation point* as the geographical point at which the telephone company's network interconnects with customer premises wiring. As previously discussed, in telephone networks this demarcation point often consists of a RJ11 jack within the User Network Interface junction box. We propose that a demarcation point should be defined not only for telephone networks but for all communication services and that this point consist of a standardized interface. A law should contain the following provision.

Demarcation Point. Facilities of communications providers at, or constituting, the *demarcation point* shall consist of an interface conforming to the technical criteria published by a recognized national or international standards body.

The demarcation point could thus consist of an RJ11 jack, a coaxial cable junction, an optical jack, an RJ45 Ethernet jack, a USB port, or an air interface such as GSM, CDMA (e.g. TIA-EIA-95), LTE, or Wi-Fi. The standards bodies may include ACTA, ANSI/TIA/EIA, USB Implementers Forum, 3GPP, 3GPP2, and IEEE.

Establishing a demarcation point for all communication services helps to ensure a user's right to choose a communications provider (U3). If more than one provider offers service, users can physically switch from one provider to another by simply disconnecting their network at the demarcation point from the old provider and connecting it to the demarcation point of the new provider.

Now that we have legally defined the interconnection point between the service provider's and user's networks, we can focus on ensuring users' rights to connect devices of their choice (U1). While Part 68 ensures this right for telephone devices, our goal is to ensure this right for all communications services. Part 68 ensured this right by allowing subscribers to attach non-harmful devices. We believe this concept applies to all communication services. Harm is currently defined with wired telephone lines in mind, but the definition can be easily extended to apply to terminal equipment that is connected to the facilities of all communications providers. We propose the following legal definition, which combines the current Part 68 definition of *harm* with the current regulatory definition of *harmful interference*.

Harm. The term *harm* means electrical hazards to the personnel of providers of communications, damage to the equipment of providers of communications, malfunction of the billing equipment of providers of communications, and unreasonable degradation of service to persons other than the user of the subject terminal equipment, his calling or called party. Unreasonable degradation includes harmful interference, defined as any emission, radiation, or induction that seriously degrades, obstructs, or repeatedly interrupts a radio communication service.

Typically, ISPs are concerned with both physical harm to their networks and potential security breaches. The term *unreasonable degradation* can and should be interpreted to include security problems that result in unreasonable degradation of service

to other users, e.g. distributed denial-of-service attacks. Network management practices that use techniques short of disconnecting a device to address security problems may also be allowed under reasonable network management.

Because ISP rights to detect and interfere with illegal uses are addressed elsewhere in law, we do not consider them here.

We propose to generalize the current Part 68 right to attach non-harmful devices to all communications services using this legal provision.

Any Device. Communications equipment located on customer premises or in the possession of the user at the end of a communications link, used to permit the stations involved to accomplish the provision of communications or information services, that do not cause harm, may be directly connected to the facilities of the communications provider.

Part 68 requires certification of terminal equipment; we propose to generalize this provision by requiring that all such communications equipment either be approved by an independent body that verifies conformance with standards that prevent harm or be connected through protective circuitry. This requirement is currently met by common network devices, since they connect through standardized interfaces.

We note that an alternative approach to ensuring an any-device right may be to require standardized interfaces to the devices themselves, in contrast to our approach requiring a demarcation point and permission to use non-harmful devices. However, we believe that definition of a demarcation point has great power: it ensures an any-device right without requiring device interface standardization; it ensures a user's right to choose a communications provider; and it helps address device management issues (considered in the following).

Our legal approach thus combines the current device rights provided to telephone network users under Part 68, the new device rights of fixed broadband Internet access service users under the Open Internet Order, and current device rights of cable television users.

5. DEVICE MANAGEMENT

We now turn to the issue of device management. We wish to distinguish between devices and protocols a service provider controls, and those controlled by a user. The demarcation point defines where one network ends and the other begins. However, while we expect that a service provider will control all devices within its network, we also saw above that it is common practice for a service provider to control certain protocols of certain devices within a subscriber's network. We thus see a need for a further architectural and legal distinction that addresses control over user devices. We start with the architecture.

Cable modems and DSL modems are devices chosen by the user. However, this does not mean that the user has the unfettered right to control all aspects of the operation of these devices. As previously discussed, these modems have multiple interfaces and the ISP typically controls at least the lower three layers of the interface facing their network.

Cable and satellite television set-top boxes are also partly controlled by the communications provider. At the very least, the provider controls the lower three layers of the interface facing its network. In addition, the provider often controls many other elements of a set-top box, including menus and navigation guides.

Smartphones are also partly controlled by the communications provider. At the very least, the provider controls the lower three layers of the air interface. In addition, the provider often controls many other elements, sometimes playing the role of a gatekeeper to all applications that can be downloaded to the device.

Fig. 1. Demarcation point and user communications gateway.

This issue of control is tightly connected to users' rights to run applications of their choice, as described by right U2. This right is fairly universally expected by users of computers with Internet access. However, it has become an issue of intense debate whether users of smartphones should be entitled to such a right, as seen in part by the FCC's reluctance to extend this right to users of mobile Internet access service. As previously stated, we believe this right should apply to all communications services.

Multiple legal models apply. The issue did not visibly arise in telephone networks since it was generally assumed that users would control all devices on their side of the demarcation point. The Open Internet Order prohibits fixed broadband Internet access service providers from blocking applications. The AllVid approach allows the video provider to control the adapter (and thus control transmission, access to services, content protection, and routing), but prohibits video provider control over navigation functions including programming guides and search functionality.

In order to create a unified approach, a control point separate from the demarcation point must be defined. The demarcation point determines who is responsible for wiring, whereas the control point will determine who is responsible for device control. Formally, we propose that the control point be legally defined as follows.

User Communications Gateway. The term *User Communications Gateway* means the customer premises equipment with network layer functionality that is closest to the demarcation point.

Customer premises equipment includes all devices on the customer's side of the demarcation point; this it includes both wired and cellular telephones, gateways, and set-top boxes. The location of the demarcation point and the user communications gateway in a typical residential network is illustrated in Figure 1.

We then propose the following limit on a service provider's control.

Control. A communications provider shall be allowed control only over communication services of devices between and including the demarcation point and the communications provider's interface of the user communications gateway, unless a user gives consent otherwise.

This legal approach would allow an ISP to control layers 1 through 3 of its interface of a cable or DSL modem, as well as any layer 1 or 2 devices in between its network

and the modem. It would not allow an ISP to control layer 4 through 7 protocols, except as required for network management, without the consent of the user.⁴

No similar provisions in current law address user versus service provider control.

6. TRAFFIC MANAGEMENT

Having defined a user's legal rights to connect to a service provider's network in Section 4 and device management in Section 5, we now consider traffic management. There has been a great deal of discussion about which traffic management techniques should be considered reasonable, see e.g. Jordan and Ghosh [2010]. However, most traffic management practices are implemented on the ISP's side of the demarcation point (in the ISP's network), and we believe these practices do not affect device attachment. We thus restrict our focus to traffic management practices on the user's side of the demarcation point. Several of these practices are related to the service contract between a user and a service provider. Although many aspects of the service contract do not pertain to device attachment, some aspects of service plans affect traffic management related to devices.

Communications providers commonly use two pricing schemes. First, a provider may charge a fixed fee per unit of time for access, e.g. basic telephone service, unlimited telephone service, most residential Internet access plans through either DSL or cable, most cable and satellite television plans, and most cellular voice and data plans. Second, a provider may charge a usage-based fee, commonly a fee per unit of time or volume, e.g. per minute of telephone service, per minute of cellular voice service, and per byte charges for cellular data service. These are often combined, e.g. a cellular voice plan that charges a fixed monthly charge for a specified number of minutes and a per minute overage charge for additional minutes. In addition, service providers may charge for access to content or for higher layer services, e.g. an ISP may charge for additional mailboxes or Web page space, a cable or satellite television provider may charge for access to premium channels or pay-per-view, and a cellular provider may charge for ringtones, enhanced mailbox service, or locater service. However, these are information services, as opposed to communications services, and are thus outside the scope of this article.

Neither fixed fees nor usage-based fees for communication services are controversial. However, the possibility that a communications provider may also charge for Quality-of-Service (QoS) has been debated. Some stakeholders argue that communications providers should not be allowed to charge anyone for QoS. Other stakeholders argue that communications providers should be allowed to charge end users but not application or service providers. Finally, some argue that communications providers should be allowed to charge end users, as well as application and service providers. We have previously argued that communication providers should be allowed to charge both residential and business subscribers, but not remote application providers that do not directly connect to the communication provider's network, providing these charges are not unreasonably discriminatory [Jordan 2007]. We have also argued that communication providers should be allowed to charge peering providers for QoS. These provisions ensure a communications provider's right to charge for communications services (P1).

We now return to the task of determining which traffic management practices are reasonable. A communications provider may implement a charge and the associated limits of a service plan either through actions taken inside its own network and/or through actions taken in a subscriber's devices. As an example, ISPs often offer multiple broadband Internet access plans, which differ by the maximum upload and

⁴Reasonable network management for devices is addressed in the next section.

download transmission rates and by price; they usually limit the download rate inside ISP equipment but limit the upload rate by setting parameters in layer 2 protocols inside a subscriber's cable or DSL modem. We would expect any limits on QoS to be handled in a similar manner; in particular, upstream QoS would likely be dictated by parameters in layer 2 and 3 protocols in the cable or DSL modem, see e.g. Jordan [2011].

Our proposed legal approach to defining user versus ISP control over user devices, provides exactly the right limits to ensure this right. Communications providers can exercise control over layer 1 through 3 protocols in user devices in between the demarcation point and the communications provider's interface of the user communications gateway. This provision ensures right P1.

Our proposed legal approach to defining user versus ISP control over user devices also provides exactly the right limits to ensure a communication provider's right to implement reasonable network management (P2). Communications providers can exercise control over higher layer protocols in between the demarcation point and the communications provider's interface of the user communications gateway, if such control is necessary for reasonable network management. There is a long history in communications law of using the term *reasonable* as a qualifier on pricing and control over communications. The determination of reasonableness is usually made by the FCC. We have propose the following.

Reasonable Network Management for User Devices. A network management practice is reasonable if and only if the user has control over the use of the practice or the practice controls Quality-of-Service on the basis of reasonable payment.

We note that delineation of reasonable traffic management is a continuing area of debate, see e.g. FCC [2010a]. We believe that our proposal is consistent with FCC regulations [Jordan and Shaffer 2010].

However it should be noted that an important subset of network management practices is implemented by ISPs for purposes of network security. While we believe that the majority of such network management practices should only be considered reasonable if the user has control over the use of the practice, e.g. by opting out if desired, we do believe this is an important area for continued research and debate.

Finally, we address the remaining user right: transparency (U4). There is a long history of encouraging transparency in various portions of communications law. The Open Internet Order included a provision for both fixed and mobile broadband Internet access service. With slight modification, we believe it can be extended to all communications services. Our proposed rule is the following.

Transparency. A communications provider shall disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections specified by user rights U1, U2, and U3.

7. FORBEARANCE

Finally, we consider a communications provider's right to forbearance from regulations when they are not necessary to ensure user rights. Title I of the Communications Act instructs the FCC to forbear from applying regulations if, (1) enforcement is not necessary to ensure that charges, practices, classifications, or regulations in connection with the telecommunications carrier or telecommunications service are just and reasonable and not unjustly or unreasonably discriminatory, (2) enforcement is not necessary for the protection of consumers, and (3) forbearance is in the public interest.

Determination of these conditions is in the purview of the FCC. We expect that the transparency requirement would always be in the public interest. We expect that the generalization of Part 68 regulations to all communications services would likely be in the public interest in nearly all situations since conformance comes at little cost or restriction to innovation, and therefore that forbearance from this provision would be rare. Similarly we expect that the enforcement of a user's right to run applications of their choice would likely be in the public interest in nearly all situations for similar reasons, and thus that forbearance should be similarly rare.

8. SCENARIOS

In this section, we revisit the technologies and regulatory models from Section 2 for telephone networks, broadband Internet access, video service, and cellular networks, and discuss how our proposed legal framework would affect the services offered by each.

8.1. Telephone Networks

Our proposal is consistent with current operation of telephone networks. Our device attachment rules are generalizations of Part 68 regulations, which already require a demarcation point with a standardized interface (ensuring right U3) and ensure a user's right to attach non-harmful devices (right U1). Harm is prevented through certification of devices or of protective circuitry. In addition to these protections, our proposal addresses device management; whereas older telephone devices had few if any issues of control, newer devices may include additional protocols for which the implementation of a user's right to run applications (right U2) is valuable. Our proposal also defines reasonable traffic management for telephone networks; it is also consistent with current operation, and extensible for future more complicated devices.

8.2. Broadband Internet Access

Our device attachment rules are consistent with current operation of cable and DSL modems. These architectures generally use junction boxes containing standardized interfaces, and thus satisfy our proposed rules on demarcation points. Our rules would simply codify this practice so that users are ensured that they can easily switch providers (if an alternative exists). These architectures also allow subscribers to choose their own cable or DSL modem, as well as to attach any other non-harmful devices of their choice. Again, our rules would simply codify this practice with harm prevented through certification of compliance with standards. Our rule on device and service plan integration would require an ISP to offer broadband Internet access service without requiring the subscriber to purchase a modem from the ISP, but nearly all ISPs have migrated to this model already. ISPs control not only devices within their own networks, but also layers 1 through 3 and selected higher layer functionality (e.g. blocking of NetBIOS traffic, DHCP, and SNMP) on the their interface to the cable or DSL modem. Our proposed rules on device management allow exactly this amount of control, but ensure that ISPs do not extend their control beyond that.⁵ In particular, an ISP can control parameters within the modem that limit the upstream transmission rate to conform to the tier of service purchased by the subscriber.

However, our proposed device attachment and device management rules may more substantially affect the deployment of residential gateways by ISPs. Such gateways generally use junction boxes containing standardized interfaces, and thus satisfy

⁵In addition, our device management rules allow an ISP to control layer 1–2 bridges and switches in between the demarcation point and the modem.

our proposed rules on demarcation points. However, although users may attach non-harmful devices of their choice on their side of the gateway, ISPs differ on whether a subscriber must use a gateway provided by the ISP or whether a subscriber may substitute it with a gateway of their choice. Our proposed device attachment rules would require that a user have the choice of the gateway, so that they may select a model with desired functionality. Thus ISPs that do not support such choice, e.g. AT&T's U-Verse service, would be in violation. We do not view such ISP restrictions as reasonable, since residential gateways use standardized protocols and harm to the ISP's network can be easily prevented through certification of compliance with these standards. ISPs similarly differ with respect to management of the residential gateway. Our rules allow ISPs similar control as for cable and DSL modems, but ISPs that do not allow user control over other protocols within the gateway, e.g. AT&T's U-Verse mandatory control over DHCP and NAT for the residential network, and mandatory firewall, would be in violation; we see no justification for such limitations on user control of protocols that do not protect the ISP's network and are not required for network management.

In addition to device attachment and management rules, we have also proposed reasonable network management and transparency rules that would apply to broadband Internet access. These rules are similar to those included in the Open Internet Order, and thus do not significantly change the law with respect to broadband Internet access.⁶

8.3. Video Service

Our device attachment rules are consistent with current operation of cable television using CableCARD set-top boxes. It is usually provided from a junction box that would satisfy our demarcation point requirement. Our rules would simply codify this practice so that users are ensured that they can easily switch providers (if an alternative exists). Current CableCARD requirements ensure that these architectures allow subscribers to choose their own set-top box, as well as to attach any other non-harmful devices of their choice. Our rules would allow a cable provider to use either CableCARD or any other method that allows user choice (e.g. they can limit channel access using a standardized authentication protocol over the network instead of using a CableCARD).

In contrast, although satellite television is usually provided from a junction that would satisfy our demarcation point requirement, satellite television providers that bar subscribers from using a set-top box of their choice would be in violation of our device attachment rule. We view user choice over set-top boxes as a reasonable requirement, unless the FCC determines that this forbearance should apply.

Although the goals of CableCARD and AllVid are to allow user control over most of the higher functionality of set-top boxes, we do not see their delineation of allowed and prohibited functionality as a clear line. Our proposed device management rules would provide a clear delineation based on layering and required network management. The rules would ensure that users have access to all purchased communication services (e.g. video on demand) with their choice of devices. They would allow service providers to control the modem and to limit access to purchased services, but not to control higher layer functionality such as navigation and search. Furthermore, it accomplishes this without reliance upon proprietary adapters.

Our proposed reasonable network management and transparency rules would apply to video service in the same way they apply to Internet access. The rules look toward the day when video services are offered over the same networks and using the same technology as Internet.

⁶That said, our definition of reasonable network management does differ from that used in the Open Internet Order. In particular, it defines reasonable network management by layer.

8.4. Cellular Networks

Our device attachment rules would be consistent with the operation of cellular providers that allow users to attach devices of their choice, challenge cellular providers that restrict subscribers' use of wireless devices obtained directly from the cellular provider. Some providers claim that wireless devices are part of their network and use of devices obtained from other providers may disrupt their network. In contrast, we see the use of standardized air interface protocols as an implementation of a demarcation point. Furthermore, we believe that certification of compliance with these standardized protocols is sufficient to prevent harm to the provider's network; indeed, that devices can roam on other provider's networks is proof of this. We thus believe that our device attachment rules should apply to cellular providers (subject to forbearance).

Our device management rules may also limit some current providers' behavior. Cellular providers that limit the functionality or applications run on wireless devices on their network would find that such limits are only allowed to the extent that they constitute required network management. Blocking of applications would be prohibited, but limits on the bandwidth used by a device would be allowed. Cellular providers would be allowed to control the air interface, but not to serve as application gatekeepers. Our rules would thus extend some of the Open Internet protections for fixed broadband Internet to mobile broadband Internet.

Finally, our proposed reasonable network management and transparency rules would apply to cellular service in the same way they apply to Internet access. The rules thus apply to smart phones in the same way they apply to wireless devices used in a residence to connect to the Internet.

9. CONCLUSION

Current legal and regulatory approaches to device attachment cannot survive technology convergence. We have proposed provisions of communications law that could ensure user rights to attach devices and to run applications, while simultaneously ensuring communications service provider rights to charge for communications services and to use reasonable network management. The provisions are designed to ensure these rights, and to be applicable in a unified manner to telephone networks, Internet access, cable and satellite television service, and cellular networks. Central to our approach is the delineation between user and provider networks via a standardized demarcation point, and delineation between user and provider control over user devices via a user communications gateway. We have illustrated how these proposed regulations would affect the services currently offered on telephone networks, Internet access, cable and satellite video networks, and cellular networks. These proposed regulations are not complete; in particular it remains to address content protection and other issues of information services.

Further research is warranted before any attempt to implement such a legal framework in communication law. First, we would like to see communications economics researchers attempt to determine the economic advantages and disadvantages of various legal approaches to device attachment. Second, we would like to hear a public policy debate over the most socially beneficial approach. Third, enforcement of any statute and regulation must be considered.

REFERENCES

- FCC. 1968. FCC 68-661, Carterfone Order.
- FCC. 1975. Part 68 Connection of terminal equipment to the telephone network. *Code of Federal Regulations, Title 47, Chapter 1, Part 68*. <http://ecfr.gpoaccess.gov>.
- FCC. 2002. FCC 02-77, Cable modem service order. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-77A1.pdf.

- FCC. 2005a. FCC 05-150, Internet over Wireline Facility Order. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-150A1.pdf.
- FCC. 2005b. FCC 05-151, Internet policy statement. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.
- FCC. 2007. FCC 07-132, AWS service order.
- FCC. 2009. FCC 09-93, Open Internet NPRM. (October). http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf.
- FCC. 2010a. DA-10-1667, Further inquiry into two under-developed issues in the open Internet proceeding. (September). http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-1667A1.pdf.
- FCC. 2010b. FCC 10-201, Open Internet order. (December). http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.
- FCC. 2010c. FCC 10-60, Allvid notice of inquiry. (April).
- François Bar and Christian Sandvig. 2000. Rules from truth: Communication policy after convergence. In *Proceedings of the 28th Telecommunications Policy Research Conference*.
- Robert W. Hahn and Robert E. Litan. 2007. The myth of network neutrality and what we should do about it. *Intern. J. Commun.* 1, 595–606.
- Scott Jordan. 2007. A layered network approach to net neutrality. *Intern. J. Commun.* 1, 427–460.
- Scott Jordan. 2009. Implications of Internet architecture upon net neutrality. *ACM Trans. Internet Technol.* 9, 2, 1–28.
- Scott Jordan. 2011. Traffic management and net neutrality in wireless networks. *IEEE Trans. Netw. Service Manag.* 8, 297–309.
- Scott Jordan and Arijit Ghosh. 2010. A framework for classification of traffic management practices as reasonable or unreasonable. *ACM Trans. Internet Technol.* 10, 1–23.
- Scott Jordan and Gwen Shaffer. 2010. Comments of Scott Jordan and Gwen Shaffer before the Federal Communications Commission in the matter of further inquiry into two under-developed issues in the open Internet proceeding. GN Docket No. 09-191 and WC Docket No. 07-52. (October).
- Scott Jordan and Gwen Shaffer. 2011. A proposed device attachment statute for converged networks. *J. Inform. Policy* 1, 394–424.
- Scott Jordan and Gwen Shaffer. 2012. Should users be entitled to use and control the devices of their choice on networks? In *Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*.
- Lawrence Lessig. 2001. The Internet under siege. *Foreign Policy* 127, 56–65.
- Lawrence B. Solum and Minn Chung. 2003. The layers principle: Internet architecture and the law. U. San Diego Public Law Research Paper No. 55. <http://ssrn.com/abstract=416263>.
- U.S. Congress. 1996. S.652.PP, Telecommunications Act of 1996, 104th Congress, Public Law 104–104. <http://thomas.loc.gov/cgi-bin/bdquery/z?d104:s.00652>.
- Kevin D. Werbach. 2002. A layered model for Internet policy. *J. Telecomm. High Technol. Law* 1, 37–67. <http://ssrn.com/abstract=648581>.
- Richard S. Whitt. 2004. A horizontal leap forward: Formulating a new communications public policy framework based on the network layers model. *Fed. Commun. Law J.* 56, 587–672.
- Tim Wu. 2007. Wireless Carterfone. *Intern. J. Commun.* 1, 389–426.

Received August 2012; revised December 2012, May 2013; accepted June 2013