Principles of Device Attachment and Control

Scott Jordan
Department of Computer Science
University of California, Irvine

Gwen Shaffer
Department of Journalism and Mass Communications
California State University, Long Beach

***Abstract*—An evolving issue of net neutrality concerns whether users should have a right to connect and control devices of their choice. In cable and satellite television networks, cellular networks, and some broadband Internet networks, the service provider often only allows use of set-top boxes, smart phones, and residential gateways obtained directly from the provider. We review how communications law currently addresses the right of a user to connect devices of their choice. We propose a set of user and service provider rights that should guide development of new legal principles.**

I. Introduction

Networking researchers often assume that users should be able to connect devices without requiring prior permission of an Internet Service Provider (ISP). In the early broadband era, ISPs often prohibited in a residential user's terms of service the connection 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. 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 protocols the devices a user places in a residential network or attaches to the Internet. The decision of which protocols of which devices are controlled by the user versus the ISP 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. 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. In the United States, users ability to attach devices of their choice to the telephone network is guaranteed by law, 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.

In this paper, we propose user and provider rights that can be used to construct a legal framework for device attachment to the Internet. The framework ensures users the right to connect devices of their choice while simultaneously ensuring network providers the right to reasonable network management. 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.

While this paper focuses exclusively on the relationship between devices and ISPs, we acknowledge that the owners of mobile operating systems are also responsible for imposing significant restrictions on devices and applications. While the proposed user and provider rights may be applied in some manner to operating systems, this study examines only actions taken by communications providers. Thus, this paper does not address device restrictions imposed by operating systems or content providers.

The problems addressed in the paper 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. However, establishing these concepts in statutory language would differ by county, and this paper only places it within the context of current United States law.

This work has been supported by the National Science Foundation.

II. Current Regulation

A. 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. In 1968, the FCC decreed that telephone companies must allow users to attach devices, providing that the devices do not harm the network [1]. The FCC developed regulations to detail the requirements for device attachment to telephone networks. These regulations, 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. A subscriber of telephone service has the right to use devices that 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.

B. Broadband Internet access

Residential broadband Internet access in the United States is most often provided via a DSL or cable modem. DSL modems are an attachment to the telephone network. DSL modems are certified not to cause harm to the provider's network, primarily by certifying that they follow standard protocols such as ADSL. Cable modems are an attachment to a cable television network. Although there is no mandated demarcation point, all wiring and devices on the customer's side of the junction between the cable company's network and the user's network serves 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.

However, unlike voice telephone network devices, the ISP controls a portion of the DSL or cable modem. Access to the particular broadband Internet service purchased by the subscriber is often implemented by the ISP controlling parameters within the DSL or cable modem. For instance, the ISP may limit the maximum upload transmission rate to a rate specified by the user's subscribed plan, block NetBIOS traffic from the user's residential network to the ISP's network, control DHCP, and operate SNMP. The ISP usually controls the operation of layers 1 through 3 and certain elements of layers 4 through 7 of the ISP's side of the cable modem, while the user controls all layers of the side of the DSL modem facing the user's residential network.

Until recently, users had no legal right to attach devices to broadband Internet access networks, and ISPs had the legal right to restrict broadband user devices. Today, limitations on user devices are rare, but examples exist, e.g. 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; we discuss this issue below. In December 2010, the FCC issued the Open Internet Order [2]. This order 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.

C. 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 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 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. 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.

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, in part because CableCARDS did not allow access to two way services such

as video on demand. In response, the FCC is considering replacing CableCARD with a new regulatory model called AllVid [3], which 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. Users would have the right to attach devices of their choice on the residential network side of the adapter.

D. 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 lock them. Each provider uses standardized air interface protocols, e.g. GSM or CDMA. 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.

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. 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. 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. 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 signalling 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.

III. User and provider rights

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

Users should have the following rights:

- 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 [4] 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 providers, application and service providers, and content providers. Right U4 is modeled on transparency principles later proposed by the FCC and many stakeholders.

Communication providers should have the following rights:

- 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 [5], 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 which specifies the conditions under which any communications regulation should be exempted; exemptions are generally granted when a marketplace is viewed as sufficiently competitive.

IV. Application of rights to technologies

A. Telephone networks

The proposed rights are consistent with current operation of telephone networks. Many are generalizations of Part 68 regulations, which 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 proposed rights address 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.

B. Broadband Internet access

The proposed rights are consistent with current operation of cable and DSL modems. Since these architectures generally use junction boxes containing standardized interfaces, they allow subscribers to choose their own cable or DSL modem, as well as to attach any other non-harmful devices of their choice (right U1); use of standardized protocols ensures user-chosen devices do not harm the network. Standardized interfaces also support a competitive marketplace for providers (right U3), if there are multiple providers.

Unlike in telephone networks, users do not have absolute control over their devices. ISPs are allowed to control not only devices within their own networks but also layers 1 through 3 (e.g. to limit the upstream transmission rate to conform with the tier of service purchased by the subscriber) and selected higher layer functionality (e.g. blocking of NetBIOS traffic, DHCP, and SNMP) on the interface on their side of a DSL or cable modem, consistent with the proposed ISP right to reasonable network management (right P2). However, use of standardized protocols in cable and DSL modems do not allow ISPs to control other elements of DSL and cable modems or other user devices, which ensures users the right to run applications of their choice (right U2).

More recently, however, 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 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 side 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 requires the subscriber to use a residential gateway it provides. 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.

Our proposed rights would require that a user have choice of the gateway, so that they may select a model with the functionality these desire. 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 are reasonable, since residential gateways use standardized protocols and harm to the ISP's network can be easily guaranteed through certification of compliance with these standards. ISPs similarly differ with respect to management of the residential gateway. Our proposed rights allow ISPs similar control as over 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.

C. Video service

Our proposed rights are consistent with current operation of cable television using CableCARD set-top boxes. Use of junction boxes satisfies the user right to choose a provider. 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. The proposed rights 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 box, satellite television providers that bar subscribers from using a set-top box of their choice would be in violation of the proposed user right to connect any legal non-harmful device. We view user choice over set-top boxes as a reasonable requirement.

Although the goal of CableCARD and AllVid is 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. We propose that reasonable network management be defined based on layering. The rules should ensure that users have access to all purchased communication services (e.g. video on demand) with their choice of devices. Consistent with DSL and cable modems and residential gateways, video providers should be allowed to control layers 1 through 3 and selected higher layer functionality of their interface to set-top boxes, but not other elements of set-top boxes or other user 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 would accomplish this without reliance upon proprietary adapters.

D. Cellular networks

Our proposed rights would be consistent with the operation of cellular providers that allow users to attach devices of their choice, but would 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.

The proposed rights may also limit some current provider's 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 proposed rights would thus extend some of the Open Internet protections for fixed broadband Internet to mobile broadband Internet.

V. Scenarios

In this final section, we explore some scenarios that have arisen in the operation of various networks and services. We ask what impact the proposed rights would have upon each scenario.

A. Device certification

CableLabs charges cable modem manufacturers $75,000 to conduct tests ensuring their devices comply with FCC standards. Even so, in Fall 2010 Comcast established its own cable modem testing requirement and began charging manufacturers $25,000 for certification. A lawsuit filed by Zoom Telephonics contended that Comcast's own testing requirement makes it harder for modem manufacturers to compete with the cable giant, which rents modems to its 17 million high-speed Internet subscribers. Comcast responded that it "wants to make sure devices our customers purchase at retail will work well and are safe".

Proposed user right U2 would allow users to connect any device to a communications network, absent harm. Comcast's justification for the additional testing invokes communication providers' right to reasonable network management (P2). However, we reject this latter claim. CableLabs testing verifies conformance with the communications protocols used on Comcast's cable network, and these protocols prevent harm. Part 68 regulations give users two options for ensuring that no harm is caused: to purchase devices that are certified not to cause harm, or to insert protective circuitry between the device and the demarcation point. Under our proposed rights, Comcast would not be allowed to require additional testing for modems already approved by CableLabs.

B. Device crippling

Verizon and AT&T cripple some Android devices when they subsidize the cost. Specifically, the wireless carriers replace Google with Bing as the default browser and prevent consumers from changing back. Paid Verizon apps (like Verizon Navigator) are given priority over free apps (like Google Maps Navigation). Finally, "bloatware" is layered on top of the devices.

Our proposed rights would ensure that communication users are entitled to run applications of their choice on devices (U3). However, providers are entitled to charge for communications services (P1), and the subsidy entitles the provider to place some limits on the use of the device. In this case, these two principles are in tension with one another.

Section 202 of the Communications Act provides a broad prohibition on unjust and unreasonable discrimination by common carriers. We propose that this prohibition should apply to all providers of communications services, including fixed or mobile broadband Internet access service and many services on cable and satellite networks. We see no reasonable argument against such an extension, except for issues of reasonable network management and forbearance. We recognize that our proposal to extend section 202 application to all providers of communications service concerns more than devices; however we see the requirements of section 202 as fundamental and, in light of the FCC's net neutrality order, they should apply to all communications services including broadband Internet access. Furthermore, Part 68 regulations ensures that telephone customers can attach any device to the network, provided it does not harm the network. In order to comply with our principles, we propose expanding these protections to cover users of all communications services, including cellular networks.

We now turn to current law on device subsidies. We propose that the Communications Act be revised to allow early termination fees, while placing limits on them so that they reflect

only device subsidies and other service initiation costs. We see no justification for early termination fees beyond ensuring a communication provider's right to recoup these costs. Additionally, we propose that the statute allow a communications provider to lock a device, but for the purposes of recouping a subsidy and thus only for the life of the service contract. Acceptance of the subsidy constitutes user choice, and thus entitles a communications provider to exercise control over communications and information services.

Of course, these conclusions are reliant on the offering of the same device without subsidy and with full functionality. Therefore, if AT&T and Verizon subsidized the cost of their Android devices, restricting their functionality would be acceptable according to the Communications Act revisions we propose. If users paid full-price for Android devices, however, our statute language would bar AT&T and Verizon from locking or crippling these handsets.

We believe that the combination of these provisions-application of section 202 of the Communications Act, broadening of Part 68, and new language concerning the integration of devices and service plans-will efficiently and effectively guarantee the right to users of communications services to connect legal non-harmful devices to a communications network. If adopted, these provisions would ensure a competitive marketplace for set-top boxes, handsets and all other communications devices. For instance, a cellular provider would be required to charge a lower monthly rate for subscribers who bring their own devices.

Therefore, we conclude that device crippling may be judged as reasonable discrimination, if a user accepts the subsidy.

C. Device tethering

Tethering applications allow users to connect various mobile devices to the Internet via their smartphones-essentially transforming handsets into wireless access points that multiple devices can use. Google blocks Verizon, T-Mobile and AT&T wireless subscribers' attempts to download tethering applications sold through its Android Market. Google says it is simply honoring requests from the carriers. Our principles assert users' right to connect any device to a communications network, absent harm (U2). At the same time, Verizon, T-Mobile and AT&T defend their ban on third-party tethering applications by citing communication providers' right to reasonable network management (P2).

As previously noted, we propose expanding Section 202 of the Communications Act to prohibit unjust and unreasonable discrimination by broadband Internet access service, as well as many services on cable and satellite networks. This means subscribers may run applications of their choice, including those enabling tethering. In addition, by broadening Part 68 regulations, we maintain that users possess the right to connect any device to a cellular network, so long as it does not cause harm. AT&T, T-Mobile and Verizon argue that blocking the apps fall within their right to reasonable network management. However, our principles contradict this stance. Cell phone customers should be charged based on the amount of bandwidth they consume and how quickly data is delivered, since these factors legitimately influence how a carrier manages its network. In this scenario, the carriers are restricting subscribers on the basis of an application, as well as on the device used to obtain Internet connectivity. Furthermore, all three carriers offer their own tethering services to customers willing to pay an additional $15 to $20 per month. Just like the free apps available from Android Marketplace, these tethering services increase network traffic.

Under our proposed principles, AT&T, T-Mobile and Verizon could not bar users from downloading tethering apps. Instead, subscribers should pay for the additional bandwidth these activities consume-regardless of whether they are enabled by a direct connection to the Internet or by cell phone tethering.

D. Creating a competitive market for devices

Cox Communication subscribers can now access the cable operator's entire video on demand library via a TiVo Premiere box. As part of the agreement, Cox supports the TiVo Premiere box as an optional set-top box and provides free installation for subscribers who purchase it from retail outlets such as Best Buy or from tivo.com. In this scenario, the principle stating that users maintain the right to use any device (U2) applies. There would be a violation of this right if users could only access the Cox video on demand library via a Cox set-top box. However, because the TiVO Premiere box is sold competitively, there is no violation. The principle of reasonable network management (P2) also applies, since a service provider has a legitimate right to limit distribution of content. Both principles suggest that the practice should be allowed.

We now turn to current regulations. The key question is whether such a subsidy entitles the communications provider to particular rights. Conflicting views on this issue usually arise because of integration between the device and services or content offered by the communications provider. Thus, for guidance, we look to the goals of CableCARD and its proposed replacement known as AllVid. Both of these devices allow subscribers access to paid TV content without requiring them to purchase equipment from a multichannel video programming distributor (MVPD). The FCC must assure the commercial availability of converter boxes, interactive communications equipment, and other gear used by consumers to access multichannel video programming from unaffiliated vendors.

The issue is not unique to MVPD networks. Cellular phone carriers often use subsidies as a justification for charging early termination fees, as well as for locking handsets to their networks. We believe there is some value in these arrangements. However, we also argue that the use of subsidies, early termination fees, locks, and other such methods of integration between user devices and service plans must be limited. Otherwise, FCC rules guaranteeing subscribers the right to use non-harmful devices are unlikely to result in

commercial availability of devices from vendors not affiliated with communications providers.

E. Blocking of text messages

To the surprise of cellular phone customers, wireless carriers have refused to transmit text messages in the past. Specifically, in September 2010, T-Mobile blocked text messages sent to its customers from WeedMaps.com, a service that locates medical marijuana dispensaries. In January 2010, Sprint blocked text messages sent to its customers from Catholic Relief Services, which was attempting to raise funds for Haitian relief efforts. In 2007, Verizon blocked messages sent by a pro-choice organization. After characterizing the messages as ”controversial and unsavory,” Verizon caved to pressure and ultimately allowed the texts to be delivered.

The principles to be considered for these scenarios include users' right to run applications of their choice on mobile devices (U3) and the right to transparency regarding all aspects of their communications services (U4). At the same time, network carriers contend their right to reasonable network management (P2) permits them to block text messages. We reject this latter claim on the grounds that carriers blocked messages due to concerns over content, rather than to manage traffic more efficiently. Because the carriers' decision to block text messages violates both U3 and U4, the principles suggest it should not be allowed.

A long history of encouraging transparency in various portions of U.S. communications law exists and, more recently, the Open Internet Order includes a provision for both fixed and mobile broadband Internet access service. Furthermore, the Communications Act prohibits common carriers from practicing unreasonable discrimination in connection with a communications service. We propose that the FCC expand this same concept to include mobile voice and data services, in order to comply with our user rights. Therefore, even if the communications provider disclosed the text message blocking, the practice would be prohibited by this provision. Finally, our principles assume that a communications provider shall not exercise control over communications or information services, unless such intervention is necessary for reasonable network management.

The wireless carriers' decision to block text messages violates all of these concepts and, therefore, would not be permissible under our principles.

F. Content exclusivity to devices

V-cast is a video-on-demand service and video library hosted by Verizon Wireless. Only subscribers with specific V-cast enabled handsets can download or stream content from the collection. According to our principles, users of communications services are entitled to connect the device of their choice to a network, so long as that device does not cause harm (U2). Connection of a device obtained from a vendor other than Verizon that can receive and display video streaming will not cause harm to Verizon's network, and therefore the practice of restricting content to V-cast handsets runs afoul of this right. Of course, communication providers are entitled to reasonable network management (P2). In this instance, we reject the carriers' argument because streaming specific content consumes the same amount of bandwidth regardless of which mobile device is used.

The Communications Act ensures that telecommunications carriers may interconnect with local exchange carriers. We propose expanding this concept to encompass interconnection of user and communications service provider networks. By doing so, we aim to ensure that the playing field in user devices is not tilted, and that user right U2 is protected. In addition, our principles would prohibit communication providers from requiring a service on the basis of a subscriber's device. Finally, U2 ensures that any non-harmful device may be directly connected to the Verizon network. This right is based on Part 68 rules, which guarantee the right to use any terminal equipment that does not harm the telephone network. As with previous scenarios, we propose to generalize this right to attach non-harmful devices to all communications services, including cellular networks.

Finally, federal copyright protections allows a communications provider to limit distribution of content when it comes to protecting intellectual property from unauthorized commercial reproduction. However, this limitation is not valid here because other devices could similarly implement content protection standards. Therefore, our principles would not allow Verizon to restrict access to V-cast content this way.

REFERENCES

[1] FCC, “FCC 68-661, Carterfone Order,” 1968.

[2] ——, “FCC 10-201, Open Internet Order,” December 2010, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.

[3] ——, “FCC 10-60, Allvid Notice of Inquiry,” April 2010.

[4] ——, “FCC 05-151, Internet Policy Statement,” 2005, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

[5] ——, “FCC 09-93, Open Internet NPRM,” October 2009, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf.