Research Publication No. 2004-03
2/2004

Illegal Internet Networks in the Developing World

Joshua Gordon

JEL Classification:O17, O19, O33

ILLEGAL INTERNET NETWORKS IN THE DEVELOPING WORLD

Joshua Gordon*

ABSTRACT

Enabled by falling costs associated with constructing international voice and data networks, and motivated by high fees charged by incumbents for international telecom services, illegal Internet network operators are proliferating in many developing countries. Unlicensed international data networks are commonly used by competitive local Internet Service Providers (ISPs) who do not have the means to obtain an international gateway license, and by Internet Telephony Service Providers (ITSPs) that deliver international calling services utilizing Voice-over-Internet Protocol (VoIP) technology.

Incumbent telecom operators and regulatory authorities in countries where unlicensed international networks are prevalent claim that these networks deprive local governments of badly needed revenue. However, unlicensed international network operators also offer a new, market-oriented model for bringing the developing world online. This model is not without political, economic, and legal risks. For example, illegal Internet networks pose a potential global security hazard as data transmitted over these networks can be difficult to monitor by intelligence agencies. Voice calls made using Internet telephony technology over these networks can be doubly difficult to track using existing legal intercept technology.

As evinced by a recent WTO ruling, growing recognition of illegal telecom networks may lead the international community to push governments of developing countries to adopt more liberal pricing and licensing policies and to pressure governments of developed countries to crack down on companies in their jurisdiction that partner with illegal network operators.

Keywords: Internet-via-Satellite, Telecommunications.

* Joshua Gordon serves on the Board of Directors of the Democracy Council (www.democracycouncil.org) and is a JD Candidate (2005) at Harvard Law School.

ILLEGAL INTERNET NETWORKS IN THE DEVELOPING WORLD

Joshua Gordon

Table of Contents

ILLEGAL INTERNET NETWORKS IN THE DEVELOPING WORLD

INTRODUCTION

> *All over the developing world, as antennas and satellite dishes sprout across the landscape - some of them placed there in defiance of the authorities - we can see the immense thirst for connection. Let us show we are listening*. – UN Secretary General Kofi Annan at the World Summit on the Information Society (WSIS) on December 9, 2003.[i]

Hidden by carefully planted shade trees and protected by a ring of barbed-wire fence, the gleaming twelve-foot wide satellite dish rises unexpectedly above the crumbling tenements and dirt lanes of a poor section of Lagos, Nigeria. On the other side of the continent, in Dar-es-Salaam, Tanzania, a building with its roof removed hides a similar antenna from pedestrians on the street below. In the hills outside Kingston, Jamaica, a wireless array peeps out of the forest and covertly beams data packets back into the city. Often found in the unlikeliest of places, homegrown means of accessing the Internet such as these are springing up across Africa, Latin America, and Asia to bring the digital revolution to millions - illegally.

Operated by a new generation of telecom entrepreneurs in some of the poorest countries in the world, unlicensed international telecommunications networks designed to carry Internet traffic are a thorn in the side of incumbent telecom operators even as they offer a new model for bringing the developing world online. However, this model is not without real political, economic and legal risks. Illegal Internet networks in developing countries can undermine state revenue allegedly earmarked for subsidizing an often aging traditional telecommunications infrastructure, and they can promote corruption as network operators, if detected, frequently bribe authorities in order to stay in business. Security risks posed by these types of networks pertinent to the world community include a difficulty in monitoring data and voice traffic that passes over them. Further, the blind eye or even encouragement typically given to these networks by many governments in countries with a deregulated telecom environment is causing increased tension between developed and developing countries.

In this essay, I outline the primary economic and technical underpinnings of illegal Internet networks and describe their most frequent applications. I then

discuss the potential security issues posed by illegal Internet networks, and the potential legal intercept implications of a shift away from a US-centered governance of the Internet to one dominated by the UN, a possible move that was forwarded at this month's World Summit on the Information Society (WSIS) in Geneva. I conclude by assessing the impact the WTO and other sources of pressure from the international community may have on the future of illegal Internet networks in developing countries.

Why Are Illegal Internet Networks Illegal?

Since the breakup of AT&T in the USA in 1984, followed by the deregulation of most European telecom markets, prices for international calls and, more recently, for Internet access have plummeted for users in those nations. In 1930, a three minute phone call from New York to London cost $245 in current dollars; in 1980, this call was priced at approximately $12; in 1997, following deregulation in the USA and in the UK, the price dropped to thirty-five cents.[ii] Today, with the advent of carrier-grade Voice-over-Internet Protocol (VoIP) technology, the cost can be as low as nine cents.

In many developing countries, however, incumbent telecommunications companies or an extremely limited set of operators still exercise official control over all international voice or data traffic that enters or leaves the country. Tariffs in these countries for international telecom services are often ten times or more the price of the same call or megabyte of bandwidth in the developed world. Nonetheless, demand for Internet access and international telephone calling are skyrocketing in these countries. At the same time, the real costs of building an international Internet network, from the price of the hardware to the Internet backbone access costs, have plummeted.

Because the vast majority of Internet content is stored on computers located in the US and in Europe, a connection to the outside world is critical to users in developing countries wanting to log on. Typical locations for connecting to the global Internet backbone are the USA, Europe, Japan, or Singapore. Even within a developing country, sending an e-mail or accessing a local web site can require an international connection if the two users subscribe to different Internet Service Providers (ISPs) due to a lack of in-country Internet exchanges. In nearly all cases, users in developing countries are obliged to shoulder the entire cost of interconnecting with the Internet backbone abroad.[iii]

In order to bridge the gulf between Internet supply and demand in the developing world, unlicensed operators of international telecommunications networks are proliferating to enable people in these countries to surf the Web and chat using Internet telephony at more affordable rates. Given their often clandestine nature, nobody knows exactly how many of these networks there are. However, their impact is wide-ranging, and can be felt even outside the developing world. In Mexico, the incumbent telecom carrier, Telmex, recently announced that illegal Internet telephony operators would cost them over $200 million in 2003 in lost revenue.[iv] Indeed, if you use a discount calling card from the US or Europe to phone Ecuador, Nigeria, or any one of dozens of developing

countries, your voice is now more likely streaming over the Internet and terminating via an illegal operator rather than traveling over conventional telephone channels.

How Are Illegal Internet Networks Used?

Illegal Internet networks are established for either or both of two purposes: 1. To provide "super-charged" Internet access to legal local ISPs as means of decreasing their reliance on expensive and often unreliable bandwidth obtained from official sources. 2. To provide the underlying network for an illegal international telephone system based on VoIP technology.

Obtaining a license to resell Internet services as a local Internet Service Provider (ISP) is not overly difficult or costly in most developing countries. Indeed, competition can be fierce in this arena in even the poorest countries. In Nigeria, for example, the number of ISPs increased from 50 in 1996 to over 270 in 2003.[v]

In order to access the Internet backbone located abroad, however, local ISPs are required to obtain an additional license to operate an international gateway, or to obtain their bandwidth from a company that has one. International gateway licenses are normally held by the incumbent telecommunications carrier, and sometimes by a handful of other providers. An international gateway license allows the company to tap into the Internet backbone via a satellite or fiber connection to a major Internet hub site nearly always located in the developed world.

International gateway licenses in developing countries are usually intentionally limited by the government, for stated reasons that include: 1. security concerns over too many international data entry points that make monitoring difficult; 2. the desire to preserve state revenues by charging expensive international gateway licensing fees, ensuring telecom services prices remain high, or protecting the licensing rights already dearly purchased by those companies which have them; or 3. preventing illegal international telephone traffic that bypasses the incumbent telecommunications operator.

Limited and expensive access to the Internet backbone in many developing countries makes the cost of Internet access, with a comparable quality of service to that in the developing world, many times more expensive than in deregulated countries. In order to keep costs at a relatively affordable level, local ISPs are obliged to greatly oversell their bandwidth. A typical oversubscription ratio in the USA is 4:1;[vi] in Kenya, for example, the oversubscription is reported to be as high as 25:1. The result is either quality Internet access priced out of the reach but all but the very wealthy, or a quality of Internet service that can be used for little besides sending occasional e-mails, Instant Messages, or very basic (and slow) web browsing.

Local ISPs in developing countries will often turn to illegal Internet access networks in order to reduce their bandwidth costs and to gain an advantage over the competition by offering a superior quality of service. They will do this by either constructing their own illegal Internet access point, or by purchasing access

from an operator of such a network. In nearly all cases, local ISPs will continue to acquire some level of Internet access from an officially licensed carrier in order to avoid raising the suspicions of authorities and to ensure a redundant bandwidth source. The nature of Internet protocol is conducive to blending multiple access routes to the Internet backbone; a series of data packets sent from one site can travel over multiple Internet routes and be automatically reassembled at the far end.

How Are Illegal Internet Networks Built?

Satellite versus Fiber

Internet data travels between countries by either cable or wireless links. Wireless Internet connections are typically created by a satellite network, which can either operate as one-way ("simplex") or two-way ("duplex") connections. Data from one location is transmitted by a satellite antenna to a satellite in geostationary orbit around the earth, which beams the signal back to a earth over a wide coverage area, where a satellite antenna on the far end receives and decodes the signal.

A simplex satellite connection, such as that for a satellite television network, ends there. In a duplex satellite connection, the satellite dish on the far end transmits a signal back to originating site, or sometimes to another dish located elsewhere.

As an alternative to satellite connectivity, fiber optic cables that are laid undersea or above ground are usually considered preferable to satellite due to the shorter distance the signal must travel before it reaches its destinations, the higher amount of data they can carry compared to a satellite network, and their tendency towards greater reliability. Cables are nearly always capable of duplex transmission.

Illegal Internet operators, however, nearly always favor satellite networking. Not only are cables are extremely expensive and difficult to construct from one country to another, but they are usually controlled by the incumbent telecom carrier or another officially licensed provider, making tapping into them illicitly nearly impossible.

A wireless connection, on the other hand, can be established nearly anywhere in the globe, using satellite antenna as small as 1.2m for a duplex Internet connection, and even smaller for a simplex connection Indeed, many developing countries do not yet have fiber connections at all, and really solely or in very large measure on satellite connectivity for all their data and voice connectivity with the outside world..

Illegal Satellite Networking: Simplex versus Duplex

Local ISPs obtain illegal bandwidth in either one-way ("simplex") or two-way ("duplex") form. The nature of most Internet traffic is asymmetrical; more data is typically received by a user than he or she sends. With a simple click by a web surfer, a very small amount of data sent 'upstream' results in the download of a relatively large web site comprised of text and graphics. As most Internet

content is on computers located outside developing countries, many satellite connections to the Internet in developing countries are set up to receive far more information than they can send in order to conserve bandwidth and reduce costs.

Technically, it is far simpler to receive Internet data from abroad than it is to transmit from a remote location. Indeed, many local ISPs are able to cheaply increase their download bandwidth by using the same kind of antenna than can be used for receiving satellite television broadcasts. These antenna tend to attract little attention from authorities, as they can be indistinguishable from satellite television dishes, which are usually legal.

However, sending data back from a developing country to the Internet backbone can be a more complicated affair. A satellite dish of considerably greater power and size is needed to transmit a data signal to outer space. Many local ISPs that use an illegal downstream Internet connection still rely exclusively on legitimate Internet bandwidth providers for their upstream traffic. As a result, the delays and packet loss experienced by Internet users from a developing country occurs due to congestion on the international upstream connection.

The quality of the upstream connection is of even greater importance when it comes to the second primary use of illegal Internet networks, international VoIP. Unlike web surfing, a digitized telephone call streaming over the Internet involves a relatively symmetrical data flow. Just as the voice of one person talking is converted into data and 'downloaded' by the listener on the other end, the other person's digitized voice must travel back 'upstream' when he or she replies. Telephone conversations carried over the Internet are particularly susceptible to quality interruptions. While it may not matter greatly if an e-mail is delayed for a second or even a couple of minutes as it travels across the Internet, a network delay of less than one second can render a telephone conversation unintelligible.

A congested upstream network is frequently the obstacle to quality VoIP calling in the developing world. Many illegal Internet networks that take on the considerable added expense and legal risk of a transmit-capable satellite dish therefore usually involve VoIP in some way.

VoIP and Illegal Internet Networks

The economics of international telephony can be compelling for an illegal Internet operator in a developing country. When most people think of VoIP, they associate people speaking through a computer. This is but one technique, and possibly the least lucrative, of how new telecom operators use VoIP in developing countries.

International Call Termination

In the most common scenario where Internet telephony is deployed by an illegal operator, the called party and the calling party may have no idea that they are using an international VoIP connection. In this model, a telephone company in a developed country will convert ordinary telephone calls from its customers into VoIP traffic that is then routed to an illegal operator in the destination country.

The operator will convert the digitized voice back into a regular telephone call, and will connect or "terminate" the call directly into the local telephone network. To the incumbent telephone company, the call will look as if it originated from within the country, and they will charge the local operator accordingly, without collecting the higher fee if the international call had come through conventional channels.

The practice of bypassing incumbent charges on international calls has been around for some time, but has skyrocketed with the advent of VoIP. Telefonos de Mexico (Telmex), the Mexican incumbent carrier, recently complained to the World Trade Organization (WTO) that illegal bypass by VoIP providers terminating their internationally-originated calls in Mexico as local calls cost it $200 million in 2003 alone.[vii]

International Call Origination

International calls originating from developing countries can be another source of significant profits for an illegal operator. VoIP operators provide international calling services to local customers through a calling card service or via an Internet-telephony equipped PC at a fixed location, often a cybercafe.

Calling card services are perhaps the most profitable forms of this business, as they enable the widest distribution. A VoIP operator will obtain local telephone lines and distribute them as calling card access numbers to his or her customers in that city or around the country. The local telephone lines are connected to a VoIP platform, which converts incoming calls to data packets and streams them over the Internet to a corresponding VoIP platform abroad. Customers phoning the local numbers will be connected via VoIP to a calling card platform located either in-country or abroad, and will terminate the call via an alternative telephone operator located outside the country. As with international bypass for incoming traffic, this type of origination scheme makes the VoIP segment invisible to the customers; to them, it appears as a normal call from one telephone to another.

Although local telephone lines obtained from the incumbent are used in this type of operation, the official international tariffs are bypassed, and the incumbent

Illegal Internet in Nigeria For Fun & Profit

A sweltering backyard in a seedy section of one of the seediest cities in all of Africa, and perhaps in all the world, is an unlikely place to find the kind of enterprise that is dramatically altering the international telecommunications landscape.

Yet from an overgrown plot in the heart of urban Lagos, Nigeria, Ayo (not his real name), an illegal Internet access operator, smuggles a remarkable amount of information between his country and the outside world. Unable to afford the astronomical cost of an international operator's license, Ayo has covertly established his own direct link to an American telecom company for high-speed Internet access.

Through this rogue international landing point, Ayo links directly to a major American telecommunications company with whom he exchanges high-speed Internet access and wholesale telephone traffic. Ayo distributes this illicit Internet connectivity to local Internet Service Providers (ISPs) starving for cheap access to the World Wide Web via a small wireless device that beams packets around the city in the public 2.4GHz radio spectrum. He also receives ordinary telephone calls bound for Nigeria made by his American partner's residential customers, which have been digitized and turned into Internet data, and plugs them directly in the city's local telephone infrastructure after decoding them back into regular voice traffic.

With six major Internet customers and nearly a quarter million telephone calls running over his system every month, Ayo pockets a princely sum for this part of the world, and boasts of profit margins that an American telecom executive would give his new Blackberry for.

Is this pirate entrepreneur concerned that he is breaking the law? Hardly. "I could go to jail, I suppose," muses Ayo. "But not if I pay the police chief a small token of my appreciation," he says with a wink. "Of course, I pay it every month. Telecom has been good to me."

collects only for the local call. The VoIP operator is able to take advantage of wholesale international rates that can be found outside the country, and which are usually dramatically lower than those obtainable from official local sources. A telephone call from Nigeria to New York, for example, can cost over $1 per minute when made through the local incumbent carrier. Over a VoIP platform connected to a telecommunications wholesaler based in London or New York, however, the cost can drop to below two cents.

International calling services that use the local infrastructure of the incumbent, but bypass official international tariffs, has been found illegal in many countries around the world. Equipment is usually confiscated, operators shut down, jailed, or heavily fined.[viii]

Internet telephony using a computer to originate the call from a developing country is commonly found in cybercafes throughout the developing world. As this method of placing the calls, known as PC-to-Phone, does not involve using the telephone lines of the incumbent at any point, this type of VoIP usage has allegedly been upheld as legal by courts in Pakistan and Panama when cases have been brought to trial.[ix]

"There is no longer a distinction between voice and data," claimed an engineer at a cybercafe in India that offered PC-to-Phone Internet calling prior to that country's deregulation of its telecom sector. "If you have one Internet connection you can talk through it, you can send e-mails, you can teleconference, whatever. What are you going to do, shut down Hotmail?"[x]

Nonetheless, even PC-to-Phone applications often involve unlicensed Internet network operators. High-speed, uncongested access to the Internet backbone is critical for enabling VoIP to work with any reasonable quality of service. As a result, even when a computer is used to send or receive international Internet telephony calls, and no part of the incumbent's traditional telephone infrastructure is utilized in making or receiving the call, Internet telephony operators will frequently turn to unlicensed sources of international Internet access to ensure the viability of their product.

The Security Issue: Legal Intercept meets Illegal Internet

Monitoring telephone calls by law enforcement agencies has been a long-standing practice in many countries, and these same authorities are increasingly on the lookout for potentially dangerous material transmitted via the Internet. In the wake of 9/11, the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) in the United States are increasingly cooperating with intelligence organizations in other countries as they jointly comb through gigantic amounts of information transmitted via telephone, fax, and e-mail through a variety of shadowy surveillance techniques, including the NSA's Echelon system and devices such as the Carnivore DCS-1000 which captures raw Internet traffic for review by authorities.[xi]

Many developing countries cite difficulties in monitoring the traffic of multiple international Internet and telephone gateways as one reason for restricting their numbers. Although many of these same countries rarely, if ever,

practice any sort of practical monitoring on the data or voice traffic that passes their borders, the concern can be a very real one.

"The developed nations must work with the developing world to counter this danger," insists Hamr, a telecommunications regulator from Egypt. "The United States should pay as much attention to the lack of monitoring on illegal networks as it has to other terrorist issues after September 11."[xii]

Indeed, traffic that passes over illegal Internet networks can be nearly impossible for the country in which the unlicensed operator is located. Although this data will certainly pass through a major Internet hub at some point in the developed world, allowing the regulators in that country to intercept it, the true country of origin may not be detectable as illegal Internet access often appears as a direct extension of the Internet backbone network it connects to.

Monitoring VoIP calls presents a special set of legal and technical issues that authorities in the US and other developed countries are only beginning to grapple with. Although Cisco, the largest producer of VoIP equipment in the world, is beginning to build lawful intercept technology into its routers,[xiii] the legality of tapping into conversations made using Internet telephony remains unclear in the United States and other developed countries. VoIP calls made through illegal Internet networks from developing countries can thus be doubly difficult to regulate under legal intercept laws, as the nature of the network used further compromises the ability of local or international telecom authorities to monitor voice conversations.

Internet Governance & Illegal Internet Networks: Global Security Implications

At the World Summit on the Information Society (WSIS), a UN-sponsored event held in Geneva, Switzerland in December 2003, heads of state and telecom regulators from around the world roundly criticized continued US control over Internet governance issues via the California-based Internet Corporation for Assigned Names and Numbers (ICANN), a private company which reports to the US Department of Commerce. Reflecting widespread dissatisfaction with a perception of US hegemony in cyberspace, South Africa, China, Brazil and India, all offered plans for turning control of the Internet over to the International Telecommunications Union (ITU), a UN agency.

Such a plan – which is not likely to be enacted anytime soon, if ever – envisions the Geneva-based ITU taking over most of ICANN's duties. If this occurs, a gradual shifting of the world's primary exchange point for Internet traffic from the USA to Europe could possibly result as the latter, already at a more accessible geographical location for fiber and satellite connectivity to Africa, the Middle East and Asia, also becomes the political locus of the Net.

Under this scenario, a decreasing amount of Internet traffic, including Internet telephony, may be subject to interception by US or similar intelligence authorities. Instead, more and more traffic would fall under the purview of a UN-sponsored approach to security and Internet monitoring.

According to French Prime Minister Jean-Pierre Raffarin, a UN Internet regime would need to guarantee "network security" and "deal with content" while at the same time "respecting freedom (of expression)."[xiv] Further details on how, or if, the UN would enact legal intercept policies for Internet traffic are far from clear. However, there is little reason to believe that any monitoring regime the UN implements will square perfectly with the expectations or current practices of US or other intelligence agencies.

On the other side of the coin, many in the international community voice concerns that UN governance of the Internet could make it easier than ever for individual countries to restrict freedom of expression over the Internet. Indeed, while the resolution that emerged from the WSIS highlighted the need for freedom of expression, it also contained language that would allow any country to restrict the flow of information on the Net for "overriding national concerns."[xv]

Indeed, the issue of security monitoring versus censorship is a delicate one, as countries define these subjects in very different ways. A website that celebrates the Dalai Lama or Taiwanese independence, for example, is to a Chinese regulator just as legitimate a subject of monitoring and suppression as an Al Queda chat room can be to his American counterpart.

Traffic traveling on illegal Internet networks may thus become subject to even less scrutiny by intelligence officials while falling victim to political censorship in individual countries more frequently. One thing seems clear: a move to governance of the Internet by a UN body is doubtless to further aggravate the political fault lines between many developed and developing countries.

International Cooperation on Illegal Internet Networks: North versus South?

Illegal Internet network operators would not be in business without willing international partners. Especially since the telecom bust of the last few years, there have been no lack of global network providers seeking to offer extremely competitive pricing to customers in any market. Vendors to illegal network operators in developing countries reportedly include the biggest names in the satellite services industry: PanAmSat, NewSkies, SingTel, and Lockheed Martin. Since the company's privatization in 2001, even Intelsat, the grandfather of all satellite companies and formerly owned jointly by over 100 member countries around the world, is said to provide service to a variety of operators in developing countries with a general disregard to their licensing status.

For these companies, providing services to network operators in countries where they may not have licensed is not seen as a problem for a simple reason: their activities are usually not deemed illegal by their home countries. Obtaining a Section 214 license from the FCC to operate as an international telecommunications carrier in the United States, for example, is a straightforward process that involves little in the way of scrutiny by government officials. Whether the customers or vendors of legal international operators in the US have a corresponding license in their home country is a subject normally viewed as being outside the jurisdiction, or at least the ability to monitor or enforce, of the FCC. As a result, state telecom authorities in developing countries regularly gripe

that their colleagues in developed countries condone the existence of illegal network operators in poor countries.

Further, the governments of deregulated countries, the US chief among them, regularly argue in international forums for the need to lower international rates for data and voice to "cost-based" pricing, while developing countries frequently strive to protect their ability to retain a high mark-up on telecommunications traffic that passes through their borders.

In the first case heard before the World Trade Organization (WTO) regarding telecommunications, the US filed a complaint in 2000 that Mexico failed to prevent the country's incumbent telecom operator, Teléfonos de México (Telmex), "from engaging in activity that denies or limits Mexico's market access, national treatment, and additional commitments for service suppliers seeking to provide basic and value-added telecommunications services into and within Mexico."[xvi] In response, Carlos Slim, the billionaire owner of Telmex, commented that "what [US authorities and telecom companies] are objecting to with Mexico is that the interconnection price is not the one they want but at the same time, it's lower than that which they pay other countries." Slim noted that Telmex had already lowered its interconnection rate from 77.9 cents per minute to 9.5 cents since 1990. [xvii]

Conclusion: Towards a WTO -Based Solution?

The initial ruling by a WTO panel on the telecommunications services dispute between the USA and Mexico issued in November, 2003, provides an indication of how the global environment for illegal Internet networks may evolve in the coming years. Although the dispute ostensibly deals only with allegedly artificially high telephone interconnection rates in Mexico and the international bypass calling practices of several US companies operating in Mexico, the WTO's treatment of the underlying issues of legal and illegal uses of the Internet likely foreshadows how the international community may address the issue of illegal Internet networks in the future.

In its November statement, the WTO panel recognized that US firms engage in the practice of bypassing Telmex's official international interconnect rates using VoIP technology, although the WTO did not address whether the underlying Internet access for these calls was obtained from legal sources. "This initial ruling is indicating that they (the United States) are the ones that did something more delicate, worse, in doing the 'bypass'," said Carlos Slim.[xviii]

In its final decision, due in early 2004, the WTO could well slap sanctions on the US for allowing American telecom companies to carry on the practice of bypass, which is illegal in Mexico. If other countries seek to apply the logic behind such a ruling to illegal Internet access points within their countries that are supplied by foreign firms, the US and other countries could be pressured into finally cracking down on companies within their borders that partner with unlicensed Internet network operators.

In the same statement, the WTO panel also called on Mexico to decrease its official international interconnection rates to levels consistent with their actual

cost. In this regard, the decision is considered, in the words of one US trade representative, "a big win for us."[xix] Indeed, sources inside the Mexican government say that a final WTO ruling that forces Mexico to lower its rates would be appealed.[xx]

By acknowledging that bypass is improper on the one hand, but on the other calling for Mexico to lower its interconnection rates and barriers to market access, the WTO is laying out a clear, if not altogether surprising solution: illegal networks should be banned, just as artificially high prices charged by incumbents and barriers to market access by would-be legitimate international gateway operators should be lowered in developing countries.

Such an approach makes good sense when applied to the problem of illegal Internet networks as a whole. For in the final analysis, illegal Internet isn't a practical long-term solution for closing the digital divide between the developing and the developed world. Governments in poor countries often find themselves expending considerable resources to police illegal operators in order to preserve state revenues, with few lasting successes to show for their efforts. In the process, authorities in developing countries repress local hi-tech enterprises and constrain the domestic deployment of viable new technologies in the process, when they should be encouraging both. By liberalizing access to small entrepreneurs operating international networks, officials in developing countries can help stimulate their often anemic economies and bolster international competitiveness, while at the same time they ensure that legal intercept regimes are enforced.

The age of monopoly profits for incumbent telcos in the developing world is rapidly drawing to an end. But given the right form of deregulation, international telecommunications networking can be a lasting – and legitimate – business for all involved.

---

[i] "Annan: Media Freedoms Must Be Reaffirmed." *Miami Herald*, December 10, 2003.
[ii] Kristof, Nicholas, "Who Went Under in the World's Sea of Cash." *New York Times*, February 15, 1999.
[iii] McLaughlin, Andrew, "Internet Exchange Points." *Global Internet Policy Initiative*, June 6, 2002. Available at: http://www.internetpolicy.net/practices/ixp.pdf
[iv] "Mexico Loses to U.S. on WTO Telecom Ruling." *Wall Street Journal*, November 26, 2003.
[v] Ovia, Jim, "Internet Service Provision in Nigeria: The Way Forward." Keynote Speech at the *1st Nigeria ISP Awards*, May 2, 2003. Available at: http://www.y2kpublishing.com/IspAwards/KeynoteSpeech.htm
[vi] "Pricing Your Business," ISP Business. Available at: http://www.ispwin2k.com/business/pricing3b.html
[vii] "Mexico Loses to U.S. on WTO Telecom Ruling." *Wall Street Journal*, November 26, 2003.
[viii] See, for example, "Two Japanese to be Prosecuted for Phone Scam in the Philippines." *Deutsche Presse-Agentur*, Tuesday, November 16, 1999 and "Court to Rule in Landmark Internet-to-Phone Case." *Gulf News* (United Arab Emirates), April 12, 2001.
[ix] Per Speech by Bryan Weiner, President, Net2Phone Global Services at ITU Telecom World 2003. I was unable to substantiate this claim.
[x] "A Cafe Rings Up Net Losses For India's Phone Monopoly." *International Herald Tribune*, September 6, 2000.

[xi] "What Big Ears You Have." *The Guardian*, September 14, 2002. "Will VoIP be Wire-Tap Ready?" *SecurityFocus*, December 12, 2003. Available at: http://www.securityfocus.com/news/7650
[xii] Personal interview at ITU Telecom World 2003, October, 2003.
[xiii] Declan McCullagh, "Inside Cisco's Eavesdropping Apparatus." CNet News.com, April 21, 2003. Available at: http://news.com.com/2010-1071-997528.html
[xiv] "France Calls for UN Net Control." *Agence France Press*, December 11, 2003.
[xv] "Annan: Media Freedoms Must Be Reaffirmed." *Miami Herald*, December 10, 2003.
[xvi] *World Trade Organization*, "Mexico – Measures Affecting Telecommunications Services." Document WT/DS204/1 (August 29, 2000), available at http://www.wto.int/english/tratop_e/dispu_e/dispu_subjects_index_e.htm#bkmk130
[xvii] Pablo Garibian, "U.S. Fares Worse from WTO Telecoms Ruling – Telmex." *Reuters News*, November 27, 2003.
[xviii] Pablo Garibian, "U.S. Fares Worse from WTO Telecoms Ruling – Telmex." *Reuters News*, November 27, 2003.
[xix] "Mexico Loses to U.S. on WTO Telecom Ruling." *Wall Street Journal*, November 26, 2003.
[xx] Pablo Garibian, "U.S. Fares Worse from WTO Telecoms Ruling – Telmex." *Reuters News*, November 27, 2003.