AT&T Response to the European Commission Consultation on the post i2010 priorities.

19 October 2009

Introduction

Operating globally under the AT&T brand, AT&T is a worldwide provider of Internet Protocol (IP)-based communications services to businesses and a leading U.S. provider of wireless, high speed Internet access, local and long distance voice, and directory publishing and advertising services, and a growing provider of IPTV entertainment offerings. AT&T operates one of the world's most advanced global networks, carrying more than 17 petabytes of total IP and data traffic on an average business day, the equivalent of a 2.7 megabyte music download for every man, woman and child on the planet. With operations in countries that cover 97% of the world's economy, AT&T has extensive global experience as an incumbent and a new entrant, as a fixed line operator and a mobile operator, and in the dynamic areas of converged technologies and services.

In the EU, AT&T is a competitive provider of business connectivity and managed network services in EU Member States, and a leading provider of bilateral connectivity services between the US and all the EU Member States.

AT&T welcomes the opportunity to express its views in this public consultation on the *post i-2010 - Priorities* for new strategy for European information society (2010-2015). This consultation will assist the European Commission in formulating a sound strategy for the development of the Information Society within the European Union (EU), allowing market players to invest in the infrastructures and services which will benefit both consumers and business. We therefore welcome the Commission's efforts to develop, in close cooperation with stakeholders, a comprehensive and ambitious digital strategy for Europe.

Consistent with the European Commission's guidance to respondents, AT&T will not attempt to address all the questions and issues raised in the consultation.

A high-speed and open Internet for all

AT&T fully supports the objective of a comprehensive policy approach to foster high investment levels in both fixed and mobile NGA. We agree that this is a prerequisite for Europe *"not to lag behind other parts of the world, thus maintaining a solid*

digital platform for innovation". But how to get to 100% Broadband. These are six ideas that we would be please to develop further :

1. ***Embrace the Diversity of Broadband.*** While "broadband" was originally understood by most policymakers in the late 1990s as simply a faster version of dial-up Internet access service that was based on a static, desktop-computer-centric user experience, today's broadband marketplace has evolved far beyond that limited vision. The number of platforms has grown (copper, cable, fiber, fixed and mobile wireless, and satellite); the customer base has expanded (consumers, businesses, government, and public and non-profit institutions, including schools, libraries, hospitals, and public-safety agencies); and the range of uses has multiplied exponentially (e-commerce, health-care delivery, voice and video communication, entertainment, fleet management, government services, education, job training, and many more). Indeed, broadband is not just about Internet access, nor is it limited to *human* interaction, as machine-to-machine (M2M) connections and applications rapidly proliferate (smart electric meters, wireless heart monitors, alarm systems, vehicle telemetry, inventory tracking, and more). The future *post i2010 - Priorities* should recognize and embrace *all* of these platforms, users, and services as part of the broadband ecosystem that will help ensure 100% broadband *access* and deliver the many societal benefits envisioned above that will, in turn, promote 100% broadband *adoption*.

2. ***Engage All Broadband Stakeholders.*** The *post i2010 - Priorities* are a strategy for the entire *EU*, not just those entities traditionally regulated in the Telecom and ICT world. It is therefore essential to engage a diverse collection of parties that have roles to play in achieving the 100% broadband goals discussed above: the private sector, consumers, public institutions, public-interest advocates and the EU government.

3. ***Promote Broadband Innovation, Investment, and Deployment and Jobs.*** The private sector has invested hundreds of billions of euros in broadband-enabled facilities, services, applications, and content over the last decade. The promotion of this investment has been, and should continue to be, the primary engine of broadband growth in the Europe.

4. ***Remove Impediments to Broadband Adoption.*** The *post i2010 - Priorities* must address the impediments that have kept some populations offline. The strategy must engage many stakeholders to provide training and public access to broadband services; economic assistance for the acquisition of broadband services and equipment; and incentives for the development of technology and content aimed at specific users' needs.

5. ***Encourage Maximum Utilization.*** The *post i2010 - Priorities* must encourage the deployment of more efficient, cost-effective and *smarter* broadband networks, services, applications, and content as efficiently as possible. As broadband becomes more ingrained in our everyday lives, from

web surfing to video conferencing to smart grids to e-commerce and e-government to telemedicine and beyond, networks will need to dynamically provide the performance capabilities required by the increasingly diverse array of services, applications, and content traveling over them.

6. ***Enhance Cybersecurity and Online Safety.*** Ensuring 100% broadband access and enabling 100% adoption will be an utterly wasted effort if the *post i2010 - Priorities* does not also include a robust strategy for ensuring cybersecurity and online safety. As broadband services play an increasingly instrumental role in virtually all facets of our cultural, economic, social, and governmental institutions, a secure and safe online environment is an imperative. We will focus more on Cybersecurity and Online Safety later in this paper.

Prerequisites for NGA investment

But we also believe that key prerequisites for NGA investment are missing from the questionnaire, such as the ability to effectively manage IP networks to allow for security, efficiency and innovation in the network.

In this context, it is regrettable that the consultation appears to start from a misconception of the role of 'smart', managed networks. The introduction to chapter 4 talks about the *"development of smart networks as opposed to transparent and open networks*" creating a false opposition. Indicating that smart networks are the opposite of open networks forwards a misunderstanding in the policy debate which will have serious consequences for innovation, investment and consumer welfare.

'Smart networks' are not only needed to effectively manage the rapidly increasing data traffic and cope with security and privacy challenges in an IP environment. They also offer ample opportunity for innovation, new and enhanced services and increased economic benefits for society. Any policy framework for the Internet therefore must allow network innovation and promote 'smart networks' that enable a rich diversity of tailor-made services and an optimal user experience.

Smart networks, those which are secure and efficiently managed, will be an essential of the Information Society. They will help to increase consumer choice, while preserving the open nature of the Internet. Smart networks will also allow independent content and applications providers to develop and market an even wider selection of products than the network permits them to offer today.

The EU should work towards a sound policy framework for IP broadband networks and the Internet, balancing objectives such as the openness of the Internet, competition between all actors in the value chain and network and service innovation to the ultimate benefit of citizens.

In order to avoid any misunderstanding, AT&T supports an open and transparent broadband environment. We note, however, that an actual definition of "openness" is missing from this consultation and the questions related to the development of NGA networks and services are difficult to address without a clearer understanding of what the concept of "openness" encompasses.

AT&T believes that an open Internet means that the Internet ecosystem enables consumers to exchange ideas and communicate freely, gives them freedom to access the lawful applications and content they want to use, and affords them the ability to choose and assemble packages of services and equipment that meet their needs.

However, an open Internet does not mean implementing new, prescriptive net neutrality rules. There is no reason for net neutrality regulations to be imposed as there has been no market failure. We believe that with the new powers attributed to the European National Regulators by the directive *on universal service and users' rights relating to electronic communications networks* (if adopted as voted by the EP in second reading), potential problems could be solved easily by the NRAs in case any market failure would appear.

Additionally, such proposals would undermine the European Commission's and the EU Member States most pressing objectives over the near term with this exercise: expanding deployment of broadband facilities and investment in related technologies and services in order to increase not only availability, but adoption.

AT&T agrees that the topic of universal access to the Internet remains a key policy issue. It should be debated in terms of concrete measures to improve access for citizens and find innovative solutions to connect rural and remote areas.

To enable 100% adoption and achieve the objective of "maximum utilization of broadband infrastructure and service," the Strategy must encourage the deployment of more efficient and cost-effective – *smarter* – broadband networks, services, applications, and content that can serve the many societal goals identified above as efficiently as possible. As broadband becomes more ingrained in our everyday lives networks will need to dynamically provide the performance capabilities required by the increasingly diverse array of services, applications, and content traveling over them. At the same time, the services, applications, and content that ride those networks will need to dynamically adapt to function properly on different types of networks with different performance characteristics (throughput, latency, congestion-sensitivity, etc.).

The *post i-2010 - Priorities* should foster new technologies and innovative solutions that can enable these smarter broadband networks, services, applications, and content. And it should categorically reject the misguided "dumb pipes" vision of the Internet espoused by some, which would thwart the substantial efficiencies to be gained from smarter networks, and which is therefore directly antithetical to the objective of maximum utilization.

Indeed, whatever one thinks of the "network neutrality" debates, everyone agrees on the need for continued massive investments in fibre, wireless, and other network infrastructure to increase the bandwidth available to all consumers. This substantial, new, risk-based investment is needed to extend broadband networks to more people in more places at affordable prices and to support the unprecedented growth of Internet traffic and the increasing demands of its changing traffic mix. Moreover, investment in smarter broadband networks is needed to meet the evolving needs of end users and enable innovative high-quality services. Everything done by the industry and by policymakers should be measured against this overriding objective.

Indeed, even in this economic downturn, Internet traffic continues to grow at a tremendous rate. A recent report by Cisco notes that the amount of traffic on the Internet in 2012 will be 75 times larger than it was in 2002, six times larger than it was in 2007, and four times larger than last year. The nature of Internet traffic is changing as well, placing new and increasing burdens on underlying networks.[1] To meet this growth and extend broadband universally, network operators need to make enormous new investments, but they also need to recover the costs of these investments. And, in order to be able to fund these investments, network providers need also to price their services at levels that consumers can – and are willing to – pay. Questions about network management and "who pays" play a key role in whether operators can expect to recover their costs, and therefore whether they will make the necessary investments in the first instance.

Effective network management helps an operator deliver a product that consumers want (a quality experience) at a more affordable price (by enhancing efficiency in traffic delivery). Intelligent network management techniques are particularly critical to ensuring quality of service amidst unprecedented traffic growth and increasing demands for more sophisticated applications and services, like real-time video or advanced telemedicine applications. As Internet usage patterns evolve and become more variable and bandwidth-intensive with the proliferation of high bandwidth applications and the ongoing explosion in Internet traffic, the nature of required network upgrades and the resulting impact on consumer rates will depend, in part, on the network management that network operators exercise. Intelligent networks that rely on a combination of increased capacity and more sophisticated network management techniques will result in better quality of service and lower costs.[2]

---

[1] For example, consumer video will be responsible for the majority of the traffic growth between 2007 and 2012. Cisco Systems, Approaching the Zettabyte Era, June 16, 2008. One minute of video requires 10 times the bandwidth as voice. Kleeman, Michael, "Point of Disconnect," University of California, San Diego, August 30, 2007.

[2] In fact, the Internet was never intended to be and has never been a collection of "dumb pipes." The Internet's founders specifically envisaged that the Internet would offer differentiated service capabilities, and they built those capabilities into the very structure of the Internet Protocol. And the Internet today treats various applications and content providers quite differently. For example, applications and content providers that can afford access to the content distribution networks or that can build their own such networks, enjoy marked performance advantages over rivals that cannot afford the use of such networks.

The question of "who pays" also goes directly to the issue of affordability. If broadband providers are prohibited from exploring various commercial arrangements and offering new and valuable services and capabilities to anyone but consumers, they will have no choice but to recover all of their costs from consumers. This would necessarily raise broadband prices for consumers above what they otherwise might be and artificially depress broadband subscribership, particularly on the margins and among low-income and other consumers who might be most sensitive to variations in price. This would also lessen investment in innovative new services and capabilities that might be of benefit to consumers and others in the Internet ecosystem. For these reasons, AT&T supports the conclusions of the Digital Britain Report that allowing providers to differentiate their offers is key to promoting investment and innovation and that, "provided consumers are properly informed, such new business models could be an important part of he investment case for Next Generation Access." To do otherwise would have a chilling effect on investment incentives, harm consumers, and exacerbate the digital divide.

In sum, there is no market failure that warrants a regulatory intervention in the Internet that would affect the management or pricing of network offerings, whether denominated as "net neutrality" or otherwise. To the contrary, the downside risk of such intervention would be enormous. We should not put investment and affordability at such profound risk by barring network management tools before even seeing their effect in operation or by barring new and creative commercial arrangements before even knowing what these arrangements might be or how they might operate in practice.

Enhancing Online Safety and Cybersecurity must be a critical part of the new EU Strategy

A. Cybersecurity

As anticipated before in this answer, ensuring 100% broadband access and enabling 100% broadband adoption in order to achieve a long list of societal benefits such as advancing consumer welfare, civic participation, community development, public safety, health-care delivery, energy independence and efficiency, education, worker training, private-sector investment, entrepreneurial activity, job creation, and economic growth through greater broadband access and adoption are objectives that are fundamentally dependent on the existence of safe and secure broadband networks and services. Yet online safety (ensuring a safe online experience for consumers) and cybersecurity (protecting networks and services from harm) all too often fail to receive the attention they deserve.

But these issues *must* be a core part of the new EU Strategy. Expanding broadband deployment and adoption without sufficient attention to both online safety and cybersecurity could actually make Europeans citizens *worse off* than they were with

lesser access to broadband. As consumers and businesses share more sensitive information online, as e-commerce expands on the Internet, and as more devices and equipment are connected to broadband networks, the vulnerability of, and potential harm to, everyone and everything using these networks will increase exponentially unless adequate safeguards are in place. Fortunately, there is a tremendous amount of expertise for addressing these critical issues in the private sector and in the governments. What is often lacking, however, is coordination.

Indeed, responsibilities for cybersecurity are distributed across a wide array of departments and ministries, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. The EU and national Member States need to integrate competing interests to derive a holistic vision and plan to address the cybersecurity-related issues confronting the EU. The EU needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks. And we would love to see a greater collaboration with the United States .

And while the European Commission and Member States recent emphasis on cybersecurity is encouraging, a key objective of the new EU Strategy Plan should be to promote greater collaboration and cooperation among all of these experts in furtherance of enhancing online safety and cybersecurity.

1. Cybersecurity Threats Are Growing

Cybersecurity threats are growing rapidly in number and sophistication. Some unsecured networks today can be disabled or sabotaged fairly readily, making them unavailable or worse. Attacks are cheap and relatively easy to conduct; the defensive perimeter is nearly infinite; and defensive measures are expensive. In one recent high-profile example, the country of Estonia was the subject of a coordinated botnet attack, with government and private computer systems flooded with up to a million times more data than normal. The country was effectively disconnected from the Internet, and the event has come to be known as "WWI" for "Web War 1." The consequences of a similar attack in other EU Member States could be severe. For instance, cyber-attacks have targeted critical infrastructure that all Europeans depend on, such as power plants, hospitals, and even national-defense infrastructure.

As broadband makes enormous contributions to health-care delivery, energy efficiency, e-government, public safety, and the like, it also creates new risks that must be aggressively managed. As we rely on networked, broadband facilities to support more and more "mission critical" services, we cannot help but dramatically increase both the number of potential targets of, and the potential damage from, cyber-attacks. Ensuring that networks are secure while maintaining their connectivity and openness is a core technical challenge to which AT&T and many others in the private sector devote significant resources. AT&T offers a wide variety of network-security services and capabilities, which we continuously upgrade to address new and emerging threats. For instance, AT&T doubled, and is now redoubling, capabilities to

provide global coverage to scrub traffic for denial-of-service attacks. AT&T went from one domestic scrubbing complex to multiple locations across the United States, as well as nodes in Europe and Asia. This gives us the ability to filter out attack traffic as close to the source of the threat as possible.

2. Recommendations

To address growing cybersecurity threats, the EU Strategy should endorse three actions:

1. First, security must be a top priority in government systems and therefore government procurement. The denial-of-service threat, for example, is largely overlooked in most government networks. This is a wasted opportunity to improve cybersecurity, as numerous vendors (including AT&T) offer solutions to mitigate the threat of denial-of-service attacks before they arrive on an agency's doorstep. But without a strategic emphasis to build strong cybersecurity protections into European procurement processes, those protections are unlikely to find their way into government networks and systems.

2. Second, the *post i-2010 - Priorities* should call on governments to establish an international partnership to enable real-time global coordination in addressing cyber-attacks. When a botnet is aimed at a critical asset, the servers controlling the attack are often scattered across the world. The local service provider that provides connectivity to the compromised server is often in the best position to take suitable security action, but this requires international cooperation that to date has been inadequate. Instead, coordination on incident response remains largely *ad hoc*. In the US, the National Security Telecommunications Advisory Committee ("NSTAC") recently recognized the problem and made recommendations in this regard – including development of international cyber-incident warning and response capabilities – that could be a good start for a better EU-US coordination on this issue. The continuing absence of a coordinated, scalable, international structure for response that includes all relevant stakeholders undercuts efforts to develop systemic solutions to cybersecurity threats.

3. Finally, the *post i-2010 - Priorities* should call for closer coordination between the government and network service providers. As attacks become more mobile and are perpetrated through networks of computers, the service provider has the best vantage point from which to mitigate the threat. Yet, too often, government and business security measures are designed with the service provider at arms-length, resulting in yet another missed opportunity to improve cybersecurity.

The public and private sectors can and should create structures for timely and secure sharing of cybersecurity threat and response information between government and

industry, and between and among critical infrastructures in a trusted, collaborative environment. In partnership with the private sector, the government can and should create a secure and responsive framework for identity management to ensure emergency responders access to critical infrastructure in support of cyber-attack recovery in a way that does not compromise network security. Further, in collaboration with industry, the government can and should create a comprehensive incident-response architecture embracing critical infrastructure facilities and core infrastructure services. Perhaps most importantly, the government should collaborate with industry on research and development efforts in pursuit of critical cybersecurity capabilities, and in furtherance of interoperable identity management processes between government and the private sector.

B. Online Safety

While the Internet provides innumerable social benefits and holds the promise for even broader social development, for many, concerns about online safety stand as significant barriers to more widespread use of broadband services. Consumers worry about the spread of viruses, spam, and other types of computer malware over the Internet; threats to their personal security, particularly identity theft and other forms of fraud and consumer abuse; and the need to protect minors from harmful content, contact, and conduct. A study issued just last year reported that 75% of online consumers worry about computer viruses, worms, and spyware, as well as the risk of identity theft. And according to one estimate, as many as one in five Internet-connected computers are now infected with malicious software, or malware. Security software vendor McAfee reported that in just the first three months of this year, 12 million more U.S. computers joined the ranks of the "botnets" – meta-networks of "zombie" personal computers that remote actors can surreptitiously control via malware[3]. McAfee estimates that 18% of IP addresses in the US are now part of botnets. Personal computers infected with botnets can be used to attack other networks or computers *en masse* and from seemingly trusted sources, leading to substantially greater danger to all users.

These threats to consumer safety and security cause real harm both to consumers and the economy more broadly. Even if they suffer no other harm, owners of compromised systems must pay to clean up and secure their PCs. Those who suffer identity theft often spend years attempting to restore their credit, and many lose trust in online commerce altogether. These costs add up quickly. The Conficker worm, the widely-discussed virus that turned millions of computers into botnet zombies, has already caused economic losses of more than $9 billion globally. And even this pales in comparison to the global loss of productivity caused each year by the need to cull spam from e-mail inboxes. Billions of dollars more are spent by security firms, ISPs, and large private networks in the "technological arms race" against sophisticated spammers. Financial institutions and e-commerce firms similarly lose more and more

[3] McAfee, *McAfee Threats Report: First Quarter 2009*, at 4 (May 2009), *available at* http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409_v3.pdf

each year to online financial fraud. Denial-of-service and other malicious attacks—often launched via botnets—can cut off online services or networks for hours or days at a time.

Finally, concerns over Internet safety, especially concerns about the safety of minors, serve as a deterrent for broader Internet adoption by families across the EU. The industry, of course, makes available many tools to help families protect their children online. But the evidence shows that addressing this issue goes beyond making tools available. It requires a multi-faceted and collaborative approach that begins with education and awareness and involves all stakeholders—parents, the Internet community, law enforcement, child-safety experts, teachers, researchers, public-health officials, and others. And government leadership is particularly critical to enable and promote this type of comprehensive collaboration and to advance the research and education initiatives that are required.

Therefore, the *Post i-2010 - Priorities* should identify the need for government leadership and improvements in online security and safety as a priority over the coming years. Enabling consumers to use the Internet more securely and safely will not only increase efficiency and save money, but it will directly serve the goal of increased adoption of broadband service. Consumers more trustful of doing business online are more likely to sign up for or upgrade their Internet access. And those who better understand how to protect themselves and their children from online threats are more likely to embrace broadband and utilize the tremendous opportunities that broadband offers.

One of the key elements in addressing this serious barrier to increased adoption is consumer education. For example, AT&T offers a comprehensive website that serves as a resource on malware, spam, Wi-Fi security, and other issues. This site also offers information on the wide variety of parental controls that AT&T makes available to its customers. Moreover, AT&T is involved in a number of online-safety initiatives through membership organizations such as the Family Online Safety Institute, and by sponsoring various educational initiatives offered by online-safety advocacy groups, such as iKeepSafe and Enough is Enough. In order to ensure that measures such as these have a broad impact, however, the Institutions must take a lead role in promoting them, and the *post i-2010 - Priorities* should make such educational initiatives a priority.

Parts of the framework for doing so already exist at the EU level. The *Post i-2010 - Priorities* should recognize and incorporate these developments into its recommendations, but it must also recognize the need for more comprehensive and sustained efforts. Toward that end, the *Post i-2010 - Priorities* should outline specific ways in which to advance Internet safety awareness and education and to ensure that the information is delivered and heard more broadly.

The *post i-2010 - Priorities* should engage policymakers in efforts beyond education, as well. In particular, the Plan should encourage the adoption of "best practices" by software designers and online providers. Broadband users need better and simpler

tools to protect their PCs, and policymakers should take steps to encourage the development and deployment of such tools. The expense and difficulty of maintaining up-to-date PC security often is far too taxing for the average consumer. Even if a consumer understands the threats and wants to take action, he or she might have to obtain security software from multiple vendors (anti-virus software, firewalls, malware removal tools, filtering software, etc.); distinguish legitimate security warnings from sophisticated, illegitimate malware; and monitor his or her Wi-Fi network and LAN to detect unauthorized use. Short of hiring a full-time IT security professional, there is a dearth of one-stop, one-click tools that can keep users safe online.

Conclusions

While all of the goals and policies enumerated above are crucially important to promoting the deployment of broadband facilities and the adoption of broadband services in general, they are indispensable to a thriving, publicly accessible broadband Internet in particular. More so than any other communications medium in history, the Internet has the ability to transform our society, our economy, and our way of life. To realize its full potential for "all people of the European Union," however, the Internet must be ***universal***, in that it must be available and affordable to consumers everywhere. The Internet also must be ***open***, in that the Internet ecosystem must enable consumers to exchange ideas and communicate freely, give them freedom to access the lawful applications and content they want to use, and afford them the ability to choose and assemble packages of services and equipment that meet their needs. The Internet must respect ***privacy***, so that consumers are in control of how, when, and by whom their private information is used. And the Internet must be ***safe***, so that networks and services are protected from harm and consumers are secure when they go online. By endorsing—and properly balancing—these four fundamental Internet values, the *post i-2010 - Priorities* will foster not only greater broadband deployment and use in general, but greater development of the Internet's potential as a transformative engine of economic and societal advancement.

Contact:
Karim Antonio Lesina
Executive Director, European Government Affairs
AT&T
Rue d'Arlon 25
1050, Brussels, Belgium
Tel: +32 2 234 61 42
Email: karim.lesina@att.com