NET Institute*

www.NETinst.org

Working Paper #03-10

October 2003

End-user security in mobile telecommunications:
Policy perspectives and a research agenda

Dr. Carleen Maitland

School of Information Sciences and Technology, The Pennsylvania State University

* The Networks, Electronic Commerce, and Telecommunications ("NET") Institute, http://www.NETinst.org, is a non-profit institution devoted to research on network industries, electronic commerce, telecommunications, the Internet, "virtual networks" comprised of computers that share the same technical standard or operating system, and on network issues in general.

End-user security in mobile telecommunications: Policy perspectives and a research agenda

A report for the NET Institute
October 15th, 2003

Dr. Carleen Maitland[1]
Ankur Tarnacha
Annemijn van Gorp
J. Rudi Westerveld

[1]Assistant Professor, School of Information Sciences and Technology, The Pennsylvania State University, 3A Thomas Bldg., University Park, PA 16802. Email: cmaitland@ist.psu.edu; Phone: 1-814-863-0640.

1. Introduction

The recent advances in mobile technologies have brought about increased functionality, however this increased functionality in turn increases the vulnerability of mobile networks, services and users. In such an environment supplying secure mobile services requires a high degree of coordination among a variety of industry players including equipment manufacturers, application developers, operating system developers and service providers. The scale of the challenge can be assessed by merely observing the difficulties faced by administrators of fixed organizational networks in their attempts to maintain virus-free networks in a context where the end users are to some degree under their control. In this light it is easy to imagine that providing secure services to end users in a highly decentralized public mobile network environment will certainly be a challenge. The complexity such services entail raises questions about whether or not service providers will be able to deliver and even more challenging offer security quality of service guarantees.

Whether or not secure mobile services will be offered is a function of both supply and demand. While certain measures can be taken to assist the traditional market mechanisms that face challenges when high degrees of coordination are required there may also be a role for public policy. As both a component of critical infrastructures and as a licensed use of the public spectrum with public interest obligations, there may be a basis for public policy mechanisms to be employed to facilitate the supply of such services.

In this paper we address these issues by first exploring factors affecting the supply and demand of security technologies and services. This is followed by a review of the policy context and recent developments in the U.S. and Europe. Information from these synopses are then combined with findings from our companion report "The Delft UMTS Testbed and End-user Security Features" to suggest a research agenda that if implemented will answer fundamental questions concerning the future of end-user mobile security.

2. Mobile security supply and demand

Security is researched from a variety of perspectives and is often considered a sub-field of information assurance (see Kabara 2002). When limited to the mobile real the perspective may be defined by the level of the network architecture. For example, security may be treated at the level of the public mobile network infrastructure, or alternatively at the level of the applications running on that network, or of the applications running on a mobile device. Here we are interested in mobile end-user security, which differs from broader conceptualizations of security in several important ways. From the end-user's perspective security is primarily concerned with safeguarding the handset from loss or theft, safeguarding the account from unauthorized charges and safeguarding locally and centrally stored data. End-user security and broader security

concerns intersect in a variety of ways, such as the implications of an overall network outage on centrally stored user data, however the end-user perspective leads to different conceptualizations of security problems and their solutions.

The current discourse on security tends to focus on public switched and organizational networks as this level of analysis has implications for a large numbers of users. This is true in both fixed network and mobile network security. However, as the number of personal-use mobile Internet subscribers grows end-user perspectives are likely to be of greater concern.

Current security problems can be analyzed from both a supply and demand perspective. The supply of secure mobile services requires two distinct parts. First there must an adequate supply of security-enabled software and hardware. Second, and perhaps more important, is the successful management of these assets. Currently the mobile market faces challenges in both domains (Pethia 2003).

The supply of secure network-level hardware and software has benefited from the recent attention to critical infrastructures. Although much of the critical infrastructures work focuses on fixed networks, mobile is increasingly seen as an important component in the overall communications infrastructure. This fixed network orientation has also spilled over to the organizational level where network administrators are struggling to keep their corporate information systems virus-free. However, like the critical infrastructures dialog, considerations of organizational network security are now also bringing mobile devices and applications into the picture.

Challenges of integrating a secure mobile computing environment into an organization include the increasingly decentralized nature of network management. Organizations have managed mobile devices such as laptops by establishing virtual private networks (VPNs) and these now must be extended to include a wider range of mobile devices each with their own physical characteristics (access mode, size, etc.) Furthermore, mobile security must take into account the diversity of public mobile networks (CDMA, GSM, TDMA) and the small size, power levels and capacity of some mobile terminals, as well as different use patterns. While laptop use may have evolved in such a way as to remain predominantly for business use, mobile phones even when supplied by the organization are often used for both personal and business use. Within this overall decentralized administrative environment the management of mobile devices will require a centralized and automated approach. In an organizational deployment network managers must consider both the initial deployment as well as ways to manage automated updates (Nokia 2002).

The supply of products such as mobile VPN software for organizational use faces several challenges, one of which is time to market pressure. Even when the software has an ostensible orientation toward security such as VPN software time to market pressures can create pressures that limit the level of robustness of the security solution. An even larger problem is with software that serves another purpose yet has an inherent security component (web browsers, email) (Pethia 2003).

Intricately connected to problems of mobile security supply is demand for these products and services. At the organizational level, while network administrators may be crying for increased security from vendors when it comes time to make the required trade-offs other factors such as interoperability and standardization usually win. The desire for interoperability and standardization not only competes directly against security features embedded in software but leads to networks that lack diversity and can lead to catastrophic failures (Hernan 2000).

Thus, even among network administrators the issue of security may not be a top priority vis-à-vis performance. Not surprisingly, the situation is likely worse among the highly distributed private network users who lack knowledge about the importance of security or lack the skills to operate their own systems securely.

Recommendations for overcoming the problems of security supply include matching the attention paid to ease-of-use in design with one of ease-of-secure administration. Such a shift requires greater training in security issues by engineers and software developers. However, the greatest changes in supply will occur when demand changes. One way to affect demand is for organizations to pay greater attention to patching and updating existing software, a reflection of an increased emphasis on security at the organizational level. Furthermore, if software and hardware are designed such that security features are easy to manage even the armies of under-informed users will be able to handle these and thus demand will follow (Pethia 2003).

While the discussions of supply and demand of secure applications and services most often assumes a fixed network and organizational environment many of these issues and subsequent recommendations are valid for the future of mobile security as well. As discussed in the companion report on the UMTS testbed, even in these advanced mobile systems that will face greater security challenges as the number and decentralization of users of the Internet increases, security has been a victim of time-to-market pressures. Furthermore, it may be the case that the current network and organizational-level bias in discussions of security may not transfer well to the hyper-decentralized context of security management of millions of mobile users which will be faced by public mobile network operators.

3. Public policy for mobile security

Mechanisms for increasing mobile security may also include public policy, particularly given the network characteristics of the technology and the societal implications of an insecure telecommunications system. Development of such public policy mechanisms may fall in the realm of security organizations, where the security of mobile services would represent a special case. Alternatively, such policies can be developed within organizations focused on the mobile sector, where the topic of security would represent a special case. Here we focus on the latter approach. In this section we discuss the mobile

telecommunications policy contexts and some recent policy developments in two important markets: Europe and the U.S.

3.1 European mobile security policy context

Public policy for mobile security in Europe will be developed in a dynamic context as the European Union has recently undertaken a far-reaching telecommunications policy reform. These current changes have their roots in the extensive liberalization program of the 1990s, which reached its peak on January 1st, 1998, the deadline for implementation of full competition (including voice telephony) in the telecommunications markets[2]. This legal basis for competition in addition to increasing Internet diffusion and convergence in the telecommunications, broadcasting and IT sectors, provided a foundation for developing a new view of the telecommunications sector. The new view aims to be technologically neutral such that services are treated similarly regardless of the medium used to deliver them and takes into account both infrastructure and associated services [3].

In addition to these general aims, the new policy regime also sought to provide a variety of protections for users, including increasing transparency of information, particularly on consumer tariffs and required publication of quality of service information. In the area of numbering, naming and addressing a primary goal was the extension of number portability to mobile users, while not requiring fixed-to-mobile portability. Furthermore, the new policy regime aimed to establish a balance between application of sector-specific regulation versus competition rules by making greater use of the latter, and accomplishing these tasks through greater delegation of authority to the national regulatory authorities (NRAs)[4,5].

Given these goals, the Commission established the new regulatory framework that laid out sector-specific legislation to be used during the development of competitive markets. The sector-specific legislation included the Framework Directive (2002/21/EC), which provides general direction, and four specific directives on licensing (Authorization Directive 2002/20/EC), access and interconnection (Access Directive 2002/19/EC), universal service (Universal Service Directive 2002/22/EC), and privacy and data protection (Directive on privacy and electronic communications 2002/58/EC). This

[2] See Commission Directive 96/19 of 13 March 1996.

[3] see http://europa.eu.int/scadplus/leg/en/lvb/l24216.htm

[4] Most of the European NRAs are quite young. Examples of beginning dates of operation include: OPTA (The Netherlands) August 1997; RegTP (Germany) January 1998; ART (France) January 1997; Agcom (Italy) after July 1997.

[5] The possibility of a similar trend from sector-specific regulation to reliance on antitrust law in the U.S. is suggested by Shelanski (2002).

represented a substantial simplification of the existing framework, reducing the number of legal measures from twenty to six[6].

These Directives provide merely a set of policy goals which are then interpreted and transposed into law at the national level. Member States were able to reach agreement on, and thereby increasing the chances of harmonized national laws, the following mobile issues: 1. the continued use of sector specific regulation in parallel with competition policy; 2. the need to cover all communications infrastructure and associated services and that markets needed to be defined dynamically particularly when considering obligations for access and interconnection; 3. an update to the Data Protection Directive, particularly as regards telecommunications, was needed.

Despite identifying a need for greater harmonization, the Member States did not agree on the following 6 mobile-related items. There were differences of opinion on the possible funding of NRAs via license fees as well as methods for selling spectrum and the possibility of allowing secondary trading of spectrum. There was also disagreement on a proposal to introduce two thresholds for asymmetric obligations in respect to access and interconnection (significant market power (SMP) and dominance) and whether or not number portability should be made available for mobile users. Further differences were found concerning user facilities (such as caller location for emergency calls, per call tariff transparency) and quality of service, particularly NRA intervention on quality of service issues[7].

Given these points of disagreement it is expected that transposition into national laws will result in a variety of rules across the Member States. However, even if full agreement were attained, differences in national legal systems would themselves create hurdles to a uniform implementation. For example, in some Member States including Belgium, France and Spain it was proposed that the legislation be implemented through a comprehensive new communications law, while in the Netherlands and Denmark the approach is to amend current law. Despite these differences mechanisms exist to facilitate harmonization of policies and procedures. Two examples are the

---

[6] The form of the legislation (i.e. Directives) has important consequences for the effects of these policies on the development of markets throughout the European Community. At the EC's formation five tools were developed that allow its institutions to impact on Member States' national legal systems to varying degrees. The five tools include regulations, directives, decisions, recommendations and opinions[6]. The directive is the most important legislative instrument alongside the regulation. Its purpose is to reconcile the dual objectives of both securing the necessary uniformity of Community law and respecting the diversity of national traditions and structures. Thus, the directive does not aim for unification of the law, which is the regulation's purpose, but instead its harmonization. The idea is to remove contradictions and conflicts between national laws and regulations or to gradually iron out inconsistencies so that, as far as possible, the same material conditions obtain in all the Member States. The directive is one of the primary means deployed in building the single market (Borchardt 1999).

[7] See COM(2000) 239 final, 26.04.2000, 'Results of the public consultation on the 1999 Communications Review and Orientations for the new Regulatory Framework.'

Communications Committee and the European Regulators' Group. Through these organizations it is hoped a higher degree of uniformity in instruments and remedies for resolving market problems can be achieved[8].

It is within this general mobile telecommunication policy context that mobile security policies have developed. In July 2002 the Commission fulfilled its promise to update the telecommunications data protection directive. This Directive is concerned with the processing of personal data and the protection of privacy in a more broadly defined electronic communications sector, which includes provisions for third party value-added service providers as well as providing direction for the handling of new types of data such as location-based data made possible by advanced mobile network technologies. The deadline for transposing this new Directive into national law is October 31, 2003.

The Directive establishes the basis for holding both 'electronic communication service' providers as well as the providers of the 'public communication network' responsible (within limits) for network security, which is to be provided through both organizational and technological measures. Furthermore, the document goes on to state that users must be notified of the risks of a security breach and where the providers choose not to insure against such risks the cost of doing so should also be provided.

Given the recent nature of these policies it is yet to be seen how these policies will be transposed into national law and subsequently enforced. Also at the national level many countries are adopting national security laws that may support or conflict with this telecommunications-specific version[9]. A second related development occurs in the Directive itself but is concerned with privacy. The Directive provides users with many rights concerning protection and management of their personal information. Along that vein, the Directive encourages Member States, where required, to adopt measures to ensure that terminal equipment is constructed in a way that is compatible with the rights of users to protect and control the use of their personal data. If such a measure was implemented to protect end-user's security it would certainly have far-reaching consequences.

3.2 U.S. mobile security policy context

The U.S. mobile security policy context is also significantly influenced by regulatory changes of the 1990s. The Communications Act of 1996 attempted to create a more vigorously competitive market in the mobile sector. The degree to which this has happened is assessed annually in the FCC's Annual Report on the state of competition in the Commercial Mobile Radio Services (CMRS) industry. In its current report the Commission concludes that the market is competitive. However, FCC Commissioner

[8] See COM (2002) 695 final 'The Eighth Report on the Implementation of the Telecommunications Regulatory Package.'

[9] See COM (2002) 695 final 'The Eighth Report on the Implementation of the Telecommunications Regulatory Package.'

Copps noted this conclusion was reached despite a severe lack of reliable, objective data on mobile services. Included in his call for more data he points out that quality of service statistics are lacking (Copps 2003a). From a mobile telecommunications perspective, mobile security may become a quality of service issue.

From a technical perspective the Commission is advised on mobile security issues from two bodies: the Technological Advisory Council (TAC) and the Network Reliability and Interoperability Council (NRIC). TAC consists of 33 members chosen for their professional and technical expertise and provides the Commission with scientifically supportable information on emerging technologies. The TAC addresses issues of network security, which it defines as issues related to the integrity, confidentiality of communications, and the technical enablers for the management of content rights. NRIC is comprised of telecommunications industry leaders and provides a mechanism whereby these members can make recommendations concerning network reliability and interoperability to the FCC. Its emphasis is on the public switched networks and it is currently concerned with developing measures and best practices for assessing reliability[10].

Although no recent policy developments appear to be directly related to end-user mobile security, several policies have been developed or are being considered that may have implications for end-user mobile security. The policies are related to the e911 system, to the resale market for spectrum, and service rules for advanced wireless services.

The e911 system for identifying the location of mobile callers to an emergency response center has been a focus of the mobile sector for a number of years. Now that the legal basis for releasing caller location information has been established (and appropriate revenue streams to fund the system have been identified) the service providers are trying to establish the legal basis for release of information in less common scenarios, such as calls from third parties. Also caught up in this petition for rulemaking were scenarios whereby small mobile operators did not have around the clock service personnel to help emergency response agencies resolve problems such as prank calls. In response to comments that the issues were beyond the jurisdiction of the FCC and the Department of Justice has been asked to become involved. Thus, when this issue is resolved the reach of the FCC in resolving issues related to security, although not mobile-service related security, and the mobile sector will be more clearly defined[11].

The second policy development that may have indirect implications for mobile security is the Commission's recent decision to allow a secondary market for spectrum. The

---

[10]See http://www.nric.org/

[11] See FCC RM-10715 Comment sought on petition for rulemaking on compliance by carriers with relevant statutory obligations on disclosure of customer information in 911 emergencies. June 16, 2003. Also, the legality of the release of customer-specific information to Public Safety Answering Points (PSAPs) in the course of response to 911 emergency calls is treated in some way by amendments made to the Communications Act, the U.S. Criminal Code via the Homeland Security Act of 2002 and the USA Patriot Act of 2001.

Commission describes its Report and Order adopted May 15th, 2003, as a landmark step in their evolution toward greater reliance on market mechanisms in expanding the scope of wireless services. It establishes two mechanisms for leasing: 'spectrum manager' leasing and 'de facto transfer' leasing. In the former the licensee must file notification with the Commission and the lessee is required to follow all technical and operational rules. However, the licensee would be required to maintain an enforcement role concerning issues related to Communications Act regulations and Commission rules, while for non-spectrum-related requirements directly related to offered services the lessee will be primarily responsible. Thus, end-user security could be affected by both the level of compliance of the lessee and the degree of enforcement by the licensee. In the 'de facto transfer' leasing arrangement prior approval by the Commission is required and the licensee's responsibilities as enforcer are greatly reduced[12].

The effects of this Order are likely to be far reaching and may limit the Commission's ability to deliver to end-users secure mobile networks and services. As reflected in the dissenting comments of Commissioner Michael Copps, it is unclear how the Commission will be able to fulfill their responsibility of overseeing that spectrum be used in the public interest when use of that spectrum is transferred without application to the Commission (Copps 2003b).

A third policy action that may have indirect effects on end-user mobile security is the Commission's November 2002 Notice of Proposed Rulemaking on Service Rules for Advanced Wireless Services in the 1.7 and 2.1 GHz Bands (FCC 02-305; WT Docket Number 02-353). In the NPRM they asked for comments on proposed standards for service or performance requirements. The performance requirements suggested in the NPRM were limited to coverage obligations and distribution of coverage obligations if spectrum is split up. Coverage obligations refer to requirements for providing services (without mention of quality standards for that service) to rural areas. It will be interesting to see if in light of Commissioner Copps comments, if this action results in an order that provides more data to the Commission concerning quality of service. Such an action could serve as the basis for collecting information about security-related performance of network operators.

Thus, in the U.S. there are no apparent policy developments directly related to mobile security, while there are a number of initiatives that could have long run implications for end-user mobile security. This situation is contrasted with that in Europe where the Commission has taken action to insure that end-users are guaranteed secure mobile services. However, it is yet to be seen how the Commission's intentions are transferred to national policy. As a last note it is also important to mention that in both Europe and the U.S. the approach to mobile security appears to be purely regional. As indicated by developments in the area of fixed network security, there is a greater need for

[12] See WT Docket No. 00-203 Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets; Report and Order and Further Notice of Proposed Rulemaking.

international cooperation in this area (ITU 200k2). At some point this approach must also be adopted for mobile networks as well.

4. Research Agenda

The review of issues and policy developments related end-user mobile security as well as our findings in the companion report "The Delft UMTS Testbed and End-user Security Features" raise a variety of questions. These questions relate directly to end-user security as well as to factors shaping the supply and demand of secure mobile services. The supply and demand of secure mobile services itself contains many issues including the relations among industry players and market mechanisms as well as policy mechanisms for affecting supply.

4.1 End-user security

How do end-users make use of the variety of PIN codes and passwords required to securely operate advanced mobile services?

It is unclear how control over the number of passwords and PIN codes is controlled and if coordinated efforts to control the end-user security experience are being made. Whether or not there is a coordinated effort, it is necessary to know what are the limits of end-user acceptance and management of these features. The answer to this question would also provide insight to the practicality of Pethia's (2003) suggestion that demand for secure technologies can be improved through education.

Do private mobile users make use of security functions differently from organizational users?

Many of the lessons from corporate/organizational fixed networks are being applied to corporate/organizational mobile networks. However, it is unclear how far the lessons learned in this context can be applied to the general public. Furthermore, given the dual use (business/private) of mobile phones, organizational security administrators need to be aware if such differences in behavior exist.

4.2 Supply and Demand

Industry relations and market mechanisms

How does the instability in the UMTS standard affect the supply of secure hard and software as well as secure mobile services?

Supplying security technologies will face many challenges including those related to the standard itself. First, with the instability that results from different versions of the standard and different implementation notes resulting from change requests the decision of which version to implement is a challenge. This instability is compounded by the slow

pace of development of the security features within the standard. Given these constraints how do companies supply secure technologies?

As in the desktop world, the security of mobile devices is likely to be highly dependent on the operating system. What trends in terms of concentration and alliances are visible in the mobile operating system market and what are the effects of these trends on the supply of secure mobile services?

Security is highly dependent on operating systems. As already mentioned as a finding from the testbed, the operating system is not transparent from the user perspective, while there are various mobile operating system providers. Currently, this is different from the PC market where Microsoft takes a dominant position.

The choice of technologies made available to end-users in their handsets and through network services is the result of a complex set of choices made by a variety of market players. How do the relationships between these players affect these choices and to what extent do they influence end-user security?

Security is the result of choices made by and behaviors of handset- and network equipment manufacturers, operators and the end user. The project findings already indicated the close relationship between the operator and the network equipment manufacturer, the lack of control of operators on handset availability but also the operator's control over the availability of certain security features. So it is interesting to research the influence of these relationships on resulting security features. The answer to this question should provide insight into the practicality of security policies that make the service provider or network operator responsible for the security of services.

Policy mechanisms

In the U.S. is there a legal basis for requiring certain security quality of service standards be provided by network operators or third party service providers?

Intervention by policy makers in the telecommunications industry are often justified by market concentration. However, in the mobile sector the Commission has deemed the market to be competitive which implies that the level of security of services be determined by the market. However, new policies, namely those concerned with Homeland Security, may provide a justification for interventions that will guarantee end-users secure services.

If so, will the secondary market enhance, degenerate or have no effect on security of service?

As suggested by Commissioner Copps, the Commission may have reduced its ability to insure that spectrum be used in the public interest through the establishment of a secondary market. An analysis of the incentives that licensees face for reporting

violations would provide insights as to the extent to which the Commission's ability has been reduced.

How will the policy concerning mobile security adopted by the European Commission be transposed into national law? How will the national laws vary? What mechanisms are in place to enforce such a policy?

The European Commission by its nature is not tied to the political forces of a nation and as such may be at greater liberty to pass legislation that will face problems at the national level. The extent to which Member States are willing and able to implement policies holding network and service providers accountable for secure service will shed light on the future of secure services and the role of the parties involved.

5. Conclusions

The research agenda presented above is derived from consideration of both the market and policy factors affecting the supply and demand of secure mobile services as well as the experience gained from involvement in a UMTS testbed in The Netherlands. While the latter exposed us to the realities of implementing a new network technologies and the challenges that are posed by security features the consideration of supply, demand and policy issues provides a broader picture of the future of mobile end-user security.

The result of this synthesis is the realization of the great deal of work to be done in this area. The research agenda proposed above spans from the user-behavior level to that of international telecommunications policy. Despite the broad range of issues covered each item comes back to the fundamental issue of the unique perspective of end-user security. The end-user perspective of security differs from network or system-level perspectives. It inherently combines what is technically feasible with the behavior of real users. This last piece is very important in this context as secure systems are vulnerable to their weakest link and thus end-user perspectives on security will in total play a large role in overall system security.

6. References

Borchardt, K-D (1999) The ABC of Community law. Fifth edition. European Commission Directorate-General for Education and Culture, Luxembourg: http://europa.eu.int/eur-lex/en/about/abc/abc_20.html

Copps, M.J. (2003a) "Statement of Commissioner Michael J. Copps Concurring, RE: Implementation of Section 6002(b) of the Omnibus Budget Reconcliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services" U.S. Federal Communication Commission, Washington D.C. June 26, 2003.

Copps, M.J. (2003b) "Dissenting statement of Commissioner Michael J. Copps, RE: Promoting efficient use of spectrum through elimination of barriers to the development of

secondary markets; Report and Order and Further Notice of Proposed Rulemaking (WT Docket No. 00-230)' FCC 03-113.

FCC (2003) "Eighth Annual Report on the state of competition in the Commercial Mobile Radio Services (CMRS) industry," U.S. Federal Communications Commission, Washington D.C. Report number FCC 03-150, July 14, 2003.

Hernan, S. (2000) Security often sacrificed for convenience. CrossTalk: The Journal of Defense Software Engineering Oct 2000.

ITU (2002) A collective security approach to protecting the global critical infrastructure. Document CNI/09, 20 May 2002.

Kabara, J. Krishnamurthy, P. and Tipper D. (2002) Information Assurance in Wireless Networks. Paper presented at the Information Survivability Workshop, Vancouver, BC, March 18-20 , 2002.

Nokia (2002) Managing Security on Mobile Terminals. Nokia White Paper. October 2002.

Pethia, Richard D. (2003) "Cyber Security - Growing Risk from Growing Vulnerability" Testimony before the House Select Committee on Homeland Security; Subcommittee on Cybersecurity, Science, and Research and Development, June 25, 2003.

Shelanski, H.A. (2002) From sector-specific regulation to antitrust law for US telecommunications: the prospects for transition. Telecommunications Policy **26**: 335-355.