Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 83 (2005)

Heft: 5

Artikel: Challenges : the privacy paradox

Autor: [s. n.]

DOI: https://doi.org/10.5169/seals-877142

Challenges – the Privacy Paradox

Will society be under more surveillance? Privacy is a central issue in the ubiquitous computing vision and has been identified as such from its earliest inception. Many in the research and development community clearly recognise the inherent challenge that networked devices hold for current social norms and values concerning privacy and surveillance.

A number of consumers and privacy advocates have voiced concern over the growing adoption of services based on radio frequency identification (RFID) technology.

Data Protection and Consumer Privacy

Given the capacity of RFID to track things and people, and to record a wide array of information, consumer advocates remain concerned about the potential risks RFID poses to individual freedoms and privacy protection. RFID critics argue that stores, corporations and governments could eventually use RFID to spy on individuals by accessing information on tags embedded in their clothing or other personal items.

The BBC News technology website recently reported on a consumer study indicating that a majority of people in the United Kingdom have serious privacy concerns related to RFID tags, believing that these tags can be read from a distance and thereby exposing them to unwanted surveillance. But despite the privacy concerns, many of those responding to the survey also recognized that RFID tagging could provide real benefits in the form of lower retail costs, convenience, and crime detection.

In some countries, RFID chips in ID cards and passports have been proposed as a way of improving security and streamlining procedures at airports. Human rights advocates are particularly concerned that biometric passports will facilitate global surveillance and lead to misuse or abuse of information. For example, how much of the identifying information will RFID chips contain, and will that data be secure from hackers? This is a public policy question, and some governments are now looking at ways to secure the data on the tag before introducing RFID chips in passports.

The "privacy paradox" associated with ubiquitous network societies involves three co-dependent domains:

- the technical domain, for example encryption and spyware
- the regulatory domain, for example rules on disclosure and retention of personal data and
- the sociological domain, for example blurring boundaries between public and private spaces

In the sociological domain, privacy issues are evaluated as they relate to social systems and norms and, in this respect, education and awareness about the concept of privacy are important starting points, according to the ITU workshop held in April 2005 on "Ubiquitous Network Societies".

Participants in the workshop raised specific challenges related to privacy in ubiquitous network societies such as authentication mechanisms (for example forgotten passwords or stolen identities), individual profiling (i. e. prediction or categorization of human behaviour), and unsolicited and fraudulent communication (for example spam, spim and phishing). Other concerns included surveillance, retention of data, and security.

The workshop recalled that privacy is widely recognized as a shared set of common values, and in many countries it is recognized as a human right. Privacy is also an important business consideration, especially as consumer demand and the building of consumer confidence are pivotal to any business case for ubiquitous network applications. In this respect, fears related to the social impact of new technological developments are important considerations for the mass take-up of ubiquitous network technologies and applications.

At the same time, the workshop suggested that the notion of individual privacy is not absolute and that protections must be balanced against collective interests in economic growth, business and social development, and the public interest. Resolving these issues will have a fundamental impact on the trust and confidence that consumers and citizens place in ubiquitous network societies.

In the specific context of data protection, the workshop concluded that it will be necessary to elaborate solutions based on shared principles in response to new challenges presented by ubiquitous networks and the use of sensors that otherwise might result in surveillance. Solutions are likely to entail the use of technology, regulatory, administrative and financial mechanisms and will need to cover data collection, retention and security issues.

Challenges for the Telecommunication Industry

The ubiquitous nature of information and communications will have a significant impact on the telecommunication landscape and current business practices. The hope for the telecommunication vendors and service providers is that ubiquitous communication will create new revenue streams, in particular, from machine-to-machine communications and item-level tagging. Operators are expecting greater revenue growth from data services than from voice services, on both fixed and mobile networks.

Ubiquitous technologies promise to be engines for economic growth, which is one reason that so many operators and firms are targeting this area. However, for traditional operators there is also the threat of cannibalisation of existing revenue streams. There are continuing tensions between the economics of Internet Protocol and Time Division Multiplexing (TDM) networks that will need to be addressed, together with issues of billing, quality of service, and network security. For instance, self-adaptive telephones will tend to reduce the price paid for calls without necessarily increasing their duration or number.

Advanced wireless technologies (such as Wi-MAX, Wi-Fi or the Republic of Korea's WiBro standard) were also seen to complement and build on current third generation mobile technologies.

The introduction of "always-on" pricing models will provide a significant improvement over traditional per-minute charging schemes. In the Republic of Korea, two out of the three licensees for WiBro are fixed-line operators (KT and Hanaro) that see WiBro as a way of winning back traffic that has shifted to their mobile competitors.

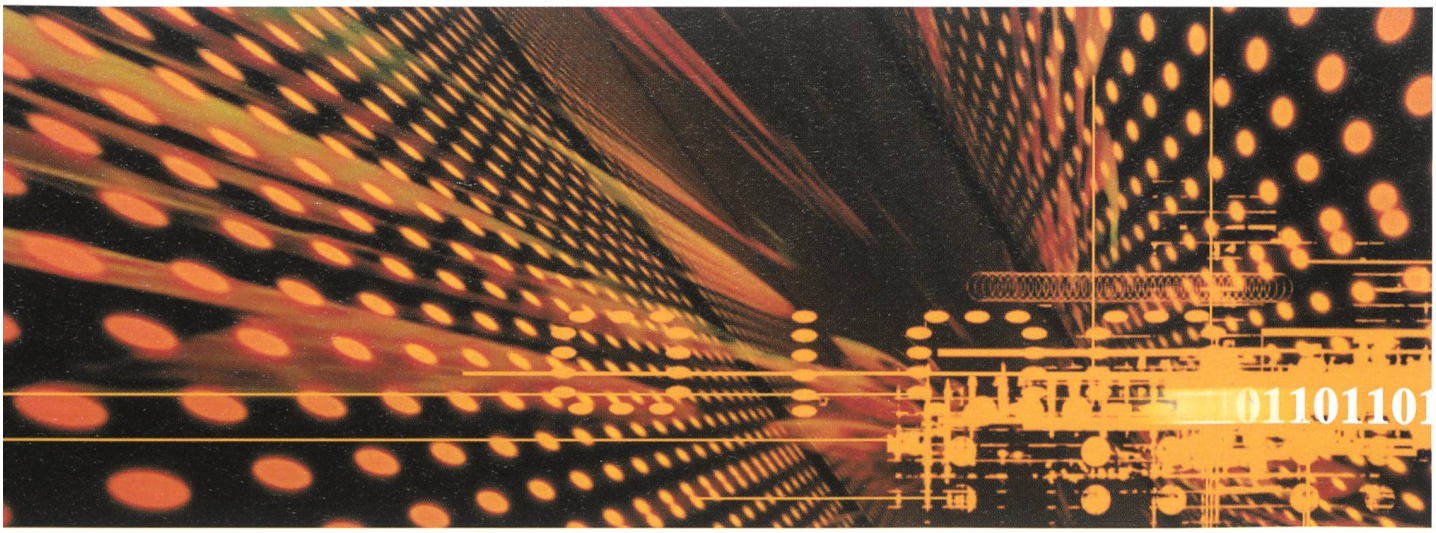
Implications for Government Policy and Regulation

The different types of service underlying ubiquitous network societies each have difficult spectrum requirements that are difficult to foresee, but certainly substantial. There also are issues around who should bear the risk and costs associated with changes in spectrum management approaches and allocation decisions. Within ITU, Working Party 8F of the Radiocommunication Sector (ITU–R) is working on the spectrum requirements of services beyond IMT-2000 (3G), with a typical radio interface of 100 to 1000 Mbit/s (depending on the level of mobility), as well as enhancements to today's 3G systems.

A market analysis of future service requirements is being undertaken in order to develop recommendations for the next world radiocommunication conference. For RFID applications, various spectrum allocations and power limitations have been agreed in different regions – for instance, 902 to 928 MHz, 2.4 watts of effective radiated power (ERP) in the United States but 868 to 870 MHz, 0.5 watt ERP in Europe. This is hindering the further development of global RFID applications and future decisions will have an impact on the structure and competitiveness of emerging markets.

New spectrum requirements for ubiquitous network societies are also posing challenges for traditional command and control or administrative spectrum allocation techniques. Some countries have already adopted market-based mechanisms for spectrum allocation (including spectrum trading in some countries) while licence-exempt services like Wi-Fi are also being deployed in a growing number of countries, creating demand for a larger spectrum "commons". Some services (for instance, public protection disaster relief) still require global harmonization. Different mechanisms for spectrum management will most likely coexist in ubiquitous network societies, and it will be important to consider whether allocation should be done on an application-specific basis or on a technology neutral one.

Government policy and regulatory issues are important considerations as ubiquitous network societies emerge. In some economies, there is a shift in focus from "e" to "u"-strategies, to reconsidering the treatment of universal service and the ubiquity of access for potentially excluded groups, including the elderly, and, potentially, to discussing new codes of social conduct. In addition, the roles of the public and private sectors in encouraging the spread of the new technologies will continue to need to be reviewed to ensure an appropriate balance in their respective contributions.



The interplay between Technological Ubiquity, Human Behaviour and Socialization

No technology can develop without an effect upon society and vice versa. The mobile phone, as an early example of a ubiquitous technology, provides an interesting case study. Mobile communication, in particular, among young people, has been accompanied by changes in social values and norms. For young people, mobile phones are regarded more as personal gadgets than as communication devices: they serve as fashion statements, as a link to their peer groups and often as a means of gaining independence from parental control. The mobile phone of the future may change radically, perhaps by being integrated into users' glasses or clothes ("invisible mobile"), accompanied by further changes in social practices. There is a need to manage increasing complexity, to ensure that functionality for users is transparent, and to develop ways of fostering trust and minimizing risk.

The real (or perceived) social consequences that may result from the global and pervasive use of ubiquitous technologies (such as RFID) will need to be considered along with the economic, organizational and political considerations, possibly in the context of multi-disciplinary global forums.

One important consideration in any assessment of these technological developments and their policy and regulatory implications (as well as the likelihood of compliance with legislative measures) is the extent to which people will remain a systemic weakness in ubiquitous network societies. Decisions with respect to the liability assigned to various human actors within these societies will play an important role in whether policy and regulatory goals can be met.

Another consideration is the development of a better understanding of the user motivations that shape demand for new applications and services and of the socio-economic factors that influence them. In particular, there is a need for ongoing discussion of the distinctive social, cultural and other values that will become embedded in the architecture of ubiquitous network societies and whether these are consistent with agreed values and ethical norms.

Shaping Ubiquity in the Developing World

One of the major factors influencing developing economy firms to adopt ubiquitous technologies is the need to meet requirements for participation in global supply chains including the requirements of their clients in the industrialized countries. For instance, the retailer WalMart, which sources many of its products from China, is progressively requiring the use of RFID tags throughout its supply chain. Although the benefits of supply-chain automation for workforce-saving may not be as significant in developing economies, the potential gains in terms of reduction of inventory losses, traceability of origin and improvements in timeliness of delivery will provide benefits. As in the case of the industrialized economies, there are issues of security, spam and privacy intrusion which may be more severe in developing economies and need to be taken into consideration, together with issues of public and private sector sources of investment.

Opportunities for international Collaboration

The development of ubiquitous, next-generation networks will require international coordination in many different areas including standardization, both of technical interfaces and product codes, frequency allocation and allocation of IPv6 addresses. As one participant in the workshop observed, "it is difficult to speak about the future, especially during a technological revolution". However, it is clear that consideration must be given to what a standards development organization in the 21st century would be like and to the priorities that should be given to global harmonization in certain areas. This will require continuous institutional evolution and, perhaps new types of mechanisms, with broader membership that could handle the many different coordination requirements, while remaining flexible, responsive and cost-effective (see www.itu.int/ubiquitous). ■

Source: ITU NEWS

Info: ITU, Place des Nations, 1211 Geneva 20, Tel. 022 730 52 34, itunews@itu.int, www.itu.int