
OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

Table of Contents

Annex A.
OECD POLICY GUIDANCE ON CONVERGENCE AND NEXT GENERATION NETWORKS

Introduction

The digitalisation of content, the emergence of IP, and the increasing adoption of high-speed broadband by end-users, has enabled the convergence of networks, services and devices we are experiencing today. These converged services often are appearing in markets as "triple" or "quadruple" play offers which provide data, television, fixed and mobile voice services. As the Internet evolves and platforms converge, it is increasingly important to ensure that end-users continue to have ready access to the Internet in a way that is supportive of the end-to-end principle.[1]

Next generation networks (NGN) are providing the platform facilitating convergence. The term "NGN" encompasses two levels of networks: *"core"* and *"access"*. NGN core networks provide the application and switching layer for a multitude of services, while next generation access networks (NGA), will facilitate the delivery of innovative services.

The convergence of a range of previously distinct applications and services, such as telephony, video, and data communications, on a single network, yields significant changes in the way networks are built and the way services delivered. The separation of distinct core network "layers" (transport, control, service and applications functions) allows for competition and innovation at each horizontal level in the NGN structure, however it may also create strong commercial incentives for network operators to increase vertical integration and might lead to the leveraging of their market power across these layers. At the same time, while new transmission networks can provide significant benefits to users in terms of capacity and bandwidth symmetry, the development of NGA may also create new barriers to competition and investment depending on the network topology and the level of investment operators require to deploy these new networks.

Policy makers and regulators may need to monitor and reassess the effectiveness of legacy policy and regulatory frameworks to reap the benefits of next generation access networks and convergence while also minimising any costs which may arise from these new developments (see the background report on *Convergence and Next Generation Networks*). Legacy policy frameworks should not hamper convergence, investment and choice in the market place. New technologies and services can bring significant benefits to end users, however policy makers may want to monitor the

1. Where the intelligence and processing power of a network reside at the outer edges while the inner network itself remains as simple as possible.

deployment of these technologies, so that the development of competition in these markets is safeguarded.

Two main objectives should be considered by policy makers in monitoring regulatory frameworks:

- Economic goals: regulation is aimed at ensuring effectively competitive markets and encouraging continued innovation and investment.
- Social objectives: many of the social objectives of existing regulatory frameworks are likely to be viewed as still valid in a new technological and service environment. These include, *inter alia*, universal service issues, access, quality of service, emergency calls, media plurality, cultural diversity and protection of consumer and other users.

This document presents a number of principles which could be used by national policy makers and regulators as a guide when addressing the ongoing challenges posed by convergence and the shift towards next generation access and core networks.

Principles

1) Market developments: encouraging investment, competition and growth

Policy makers should aim to create a favourable environment for investment and innovation and ensure a predictable legal and regulatory environment for market participants. In this context, they may want to consider a series of possible barriers to competition and investment that may arise following the deployment of NGN. There are a number of instruments to help adequately address these barriers. In particular, policy makers should:

- Recognise that policy and regulatory measures to promote competition in a next generation environment should be based on a sound economic assessment of specific market conditions and local factors.
- Recognise the need for regulators to consider possible market dominance resulting from the bundling of services.

In addition, if adequate facility-based competition does not develop, where LLU has been mandated, policy makers should:

- Consider difficulties that may arise in replicating next generation access networks which could lead to the creation of new bottlenecks for competition, which may require policy makers to take appropriate steps to ensure there is no undue discrimination in access to these networks. This is particularly relevant in countries relying on unbundling to promote competition since it may be more difficult to meaningfully unbundle next generation access networks.
- Recognise that in certain circumstances service-based competition may provide an important first step to encourage competition in the market and investment by new entrants.

- Consider the need to ensure that service and application providers have non-discriminatory access to network resources where there are limited choices for network access.

2) Access to passive infrastructure

- Recognise that as a large part of the cost of deploying fibre networks is in civil works, appropriate policies should be in place to ensure fair and non-discriminatory access to ducts, poles and rights of way. Policies should facilitate access to the ducts and poles of incumbent communication operators (wireline and wireless telephone and cable operators) and utility companies. Access to rights of way and ducts should be available on a non-discriminatory basis and on cost-based terms.
- Recognise that without adequate facility-based competition, fibre rollouts closer to users may introduce new bottlenecks such as curb-side cabinets and the inside wiring of apartment buildings. Depending on local factors, these new bottlenecks may require regulatory action such as sub-loop unbundling and sharing of optical line termination equipment points at apartments/buildings.

3) Technology-neutral regulation

Following the convergence of network and services, it is important to ensure that the market is open for different technologies to compete on equal terms. In this context:

- Governments should encourage, to the extent possible, the development of technologically neutral regulation, particularly in converged areas.
- In the cable and mobile sectors, regulators should consider where the move from technology-specific licences to service-neutral authorisation frameworks would be beneficial in terms of efficient management of scarce resources, spectrum allocation, and achievement of relevant public interest objectives.

4) Interconnection

Interconnection also plays an important role in a NGN environment because it needs to take place at all functional levels in order for all service providers to be able to access the new networks and provide their content, service and applications to end-users. Commercial markets for the exchange of IP traffic have developed well without regulatory intervention. Policy makers should therefore:

- Monitor the future development of NGN markets to encourage seamless and non-discriminatory exchange of traffic between networks, and consider where regulatory intervention is still necessary.
- Re-examine the functioning and evolution of the existing interconnection system and the evolution in the transition to NGNs through industry and user consultations.

5) Numbering, naming and addressing

IP addresses, telephone numbers, and other addresses are crucial resources for communication and access to the market. In particular, the availability of new address space is necessary for the growth of the Internet. Governments should:

- Encourage the adoption of the new version of the Internet protocol (IPv6), in particular through its timely adoption by governments as well as important private sector users of IPv4 addresses, in view of the impending IPv4 depletion.
- Review numbering plans to increase flexibility, facilitate new converged services, and improve the nomadicity of persons.
- Monitor the use of ENUM as a routing and interconnection mechanism between networks.

6) Spectrum allocation

Wireless technologies, including those using unlicensed spectrum, are becoming an important part of the telecommunications landscape. Effective spectrum management is becoming a key policy issue as the range of technologies making demands on spectrum is growing rapidly. This may require policy makers to:

- Encourage the rapid transition to digital broadcasting and make parts of the released spectrum (digital dividend) available for new and innovative wireless communication and broadcasting services.
- Reform spectrum allocation and use market mechanisms and other schemes that reflect the economic value of spectrum in spectrum markets, where feasible taking into account public interest objectives such as interoperability, promotion of cultural and linguistic diversity and media pluralism.
- Review institutional structures for spectrum planning and allocation to ensure that they are better co-ordinated with the needs of the market and with the requirements of efficient regulation.

7) Universal service

Universal service is an evolving concept that may change over the years to reflect advances in technologies and usage. Policy makers may need to review definitions of universal service to determine whether changes need to be made and, if so, what services and access would be required. They must also decide whether funding mechanisms should change. In this context, governments should:

- Review universal service obligations and the mechanisms to achieve them in the context of convergence.
- Ensure that contributions to universal service funds respect the trend towards convergence of network and services, and review how universal service is funded.

8) Digital divide

The deployment of NGN may create new asymmetries in access in areas not reached by high-speed broadband infrastructures. This can raise new concerns about regional competitiveness and economic growth.

- Governments should encourage the development of nation-wide high-speed broadband networks to avoid the creation of access asymmetries within countries, which can be particularly pronounced between urban and rural areas. In this context it is important that alternative networks are encouraged. Public-

private partnerships may provide a solution in some areas to reduce investment costs given that the cost of providing fibre to homes in rural and remote areas may be high with current prices and technologies.

9) Emergency services

There is an increased risk of confusion as to whether or not users have access to emergency call services with the convergence of platforms and devices, increased mobility and the shift to IP-based communication. Steps should be taken to:

- Ensure that users of innovative voice services are appropriately informed regarding access to emergency services and that some kind of access to emergency services is guaranteed to users of VoIP services. These provisions should also take into consideration the technical difficulties of providing such services and should not constitute an excessive burden or obstacle to the development of innovative services and applications.

10) Quality of service

Quality of service remains important in a converged next generation environment where information travels across multiple networks. In this context, policy makers should:

- Ensure that convergence benefits consumers and businesses, providing them sufficient choices with respect to connectivity, access and use of Internet applications, terminal devices and content, as well as clear and accurate information about the quality and costs of services to enable them to make informed choices.

11) Telecommunication and broadcasting convergence

Convergence allows different types of content and communication services to be delivered through the same network and consumed over a variety of platforms and user devices. The evolution of technology does not necessarily change many of the underlying social and cultural objectives but may change the way these objectives are achieved. The evolution of technology may also allow for increased market liberalisation, while maintaining core policy goals. To this end governments should:

- Reconsider existing platform-specific obligations in light of the convergence of telecommunication and broadcasting and develop cross-media policies for a multi-platform environment so as to ensure consistency of regulation.
- Facilitate the diffusion of content through different devices.

12) Cross-border issues

Governments may need to address cross-border issues as services are increasingly geographically and network independent. This creates significant challenges for policy makers. In particular, they might need to:

- Review consumer protection frameworks, content regulation measures, the protection of intellectual property rights, the protection of privacy and personal data, and legal interception.

Annex B.
OECD POLICY GUIDANCE FOR PROTECTING AND EMPOWERING CONSUMERS IN COMMUNICATION[1] SERVICES

Over the last decade, the communications sector has been subject to transformation with the development of competition and the diffusion of a range of new technologies and services. Competition has brought significant benefits to consumers with falling prices, better quality of services, a wider choice of service providers and access to new services. The technological and service developments have resulted in communications by electronic means becoming a central feature in OECD countries and this will become even more so as next generation communication infrastructures and services are put into place. The significant benefits to consumers in the development of new services and technologies has also had some costs as consumers have been faced with more complex choices, a range of offers sometimes with unclear pricing structures and contracts which at times limited the flexibility of consumers.

The emphasis on creating competition in communication markets has been mainly through supply side measures but, in recent years, there has been more recognition that informed and empowered consumers can, through demand-side choices, stimulate firms to innovate, improve quality and compete in pricing. By making well-informed choices between suppliers, consumers not only benefit from competition, but they drive and sustain it.

At the same time, as the use of communication services has increased, more emphasis is being placed on reviewing consumer policy relating to communication services by supplementing the range of consumer measures to provide better protection, more flexibility in the market for consumers, and better access to information.

It is in this context that OECD countries have developed a set of policy principles for ensuring that consumer interests in communication services are adequately protected. This guidance recognises that it is necessary to ensure transparent and effective consumer protection while maintaining an environment that provides incentives for investing in developing new communication services. In this respect, the principles in the present policy guidance should be read in conjunction with those in the 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*, the 2003 *OECD Guidelines for Protecting Consumers from*

1. By "communications," this paper refers to telecommunication service providers, Internet access and telecommunication services provided by cable TV companies and Internet service providers.

Fraudulent and Deceptive Commercial Practices Across Borders, and the 2007 *OECD Recommendation on Consumer Dispute Resolution and Redress*.

The OECD policy guidance is aimed at:

a) Encouraging the development of services that provide consumers with a range of quality products at competitive prices.

b) Informing consumers about potential security and privacy risks in using communication services and available measures to limit these risks.

c) Enhancing consumer awareness of the availability and benefits of available services and suppliers, and consumer rights.

d) Improving the transparency of contracts and ensuring that they are not unfair to consumers.

e) Minimising the costs associated with switching services.

f) Facilitating timely, inexpensive, easy to use, effective and fair settlement of consumer complaints.

g) Ensuring that services be widely accessible to everyone, and, in particular, disadvantaged and vulnerable consumers.

In this context:

The complexity of communication services, the plethora of new services and the increasing purchase of bundled services through long term contracts have made it increasingly difficult to understand and compare services.

- *Consumers of communication services should be provided by service providers with clear and accurate information about the terms, conditions and costs associated with those services; the information should be easily accessible and sufficient to enable them to make informed decisions.*

- *Developing information resources that could help consumers make informed choices and increase awareness of their rights and relevant consumer protection measures would be beneficial. In developing such resources, attention should be given to the special needs that disadvantaged or vulnerable consumers may have.*

- *Independent third parties and consumer organisations should be encouraged to provide price/service-comparison information that will help consumers make informed choices.*

The technical quality of communication services provided to consumers can vary significantly and there is concern in some countries that some operators may degrade the quality of services provided to consumers to low levels and without the knowledge of the consumer.

- *In the interest of transparency, operators are encouraged to inform consumers of the quality of services including, where practical, information on the variability in the quality of such service, to enable informed consumer choice and facilitate decisions about switching.*

The availability of emergency numbers and emergency hotlines is sometimes limited; certain emergency numbers that may be available via traditional telephone services, for examples, are not available in some countries via VoIP.

- *Access to emergency services and to emergency hotlines should be ensured without respect to the type of communication service involved. This provision should take into consideration the technical difficulties of providing such services and the limitation of services not meant to be substitute for basic voice products. The provision should not constitute an excessive burden or obstacle to the development of innovative services and applications. Any limitations in the emergency services provided should be clearly and conspicuously disclosed.*

The ability of consumers to switch service providers is often discouraged because of the time and costs involved. Lower switching costs may benefit consumers and provide a greater stimulus to operators to charge competitive prices and improve the quality of service.

- *The time and costs associated with switching services by consumers should be minimised. For example, the notice periods for ending contracts, or the "lock in" period for mobile phone handsets could be limited in order to facilitate switching.*

Number portability plays an important role in the promotion of competition by removing the cost and inconvenience of having to change telephone numbers when switching providers. It also reduces barriers for adoption of competitive offerings.

- *Number portability should be ensured and be carried out expeditiously when consumers switch providers in accordance with the numbering policy of the country.*

An absence of interoperability such that consumers need to buy new equipment to utilise another provider's service can inhibit the switching process.

- *Ways to increase interoperability, balancing this need against the need to stimulate business innovation, should be explored by stakeholders.*

Bundling can be beneficial to consumers and, indeed, an increasing number of consumers are subscribing to bundled service plans. But bundling can also be restrictive if the consumer wishes to change service provider for one service (*e.g.* voice or Internet) which would necessitate changing the provider for all services.

- *The provision of unbundled services should be considered, when necessary, to protect competition, or to preserve consumer choice, recognising that the differences in price between bundled offerings and stand-alone services are often efficient and beneficial to consumers.*

- *Access to emergency communication services should be ensured in the event that other bundled services are interrupted for non-payment.*

Communication service providers can use selling techniques that are fraudulent and misleading. Sales have, for example, been pursued through slamming; contracts can contain restrictive conditions and exemptions (download limits, restrictions to access content) that are otherwise not clearly indicated in promotional literature. Further, advertising and marketing campaigns that exaggerate or distort claims can be particularly harmful to certain categories of consumers, such as children or other

disadvantaged or vulnerable consumers who may not have the capability to fully understand the information presented.

Consistent with the 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce and the 2003 OECD Guidelines for protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders:

- *Businesses should provide consumers with clear descriptions of the details and costs of contracts.*
- *Businesses should be prohibited from engaging in any practice that is fraudulent or deceptive.*

Consumer contracts are often renewed automatically in a number of OECD countries without the explicit approval of consumers, and sometimes modification of contractual conditions are made without sufficient notice and without informing consumers about their right of withdrawal in such cases.

- *Communication service providers should be encouraged to limit initial contracts, after which a reasonable time period of notice to end the contract should be provided.*
- *The implications for consumers of "opt-in" and "opt-out" default provisions at the time of contract renewal should be further examined by stakeholders.*
- *Consumers should receive adequate notice of any intention to modify contractual conditions and about their right of withdrawal in such cases.*

Despite technological advances, inaccurate billing continues to be a major cause of consumer complaint.

- *The use of self-regulation and industry codes of practice concerning billing is encouraged.*
- *Regulatory monitoring and/or intervention may be required, in appropriate cases, to enforce consumer protections.*

Consumers may be reluctant to take legal action when they have serious disputes with their service provider, either because of the time and expense involved and/or because they find the judicial process intimidating.

- *As provided for in the 2007 OECD Consumer Dispute Resolution and Redress Recommendation, consumers should have access to fair, easy-to-use, timely, effective and inexpensive dispute resolution and redress mechanisms, including, where possible, alternative dispute resolution services.*
- *Establishing independent dispute resolution bodies dealing with communication service issues should be encouraged.*
- *Voluntary consumer representation agencies, whose functions could include assisting consumers with dispute resolution, could be encouraged.*
- *The role of regulators in dispute settlement should be made clear. The functions of regulators need to be well publicised.*

New communication services have also led to increased risks for consumers in terms of privacy and security when using networks and services. Consumers need to be aware of these risks and of the available measures that may be available to protect themselves.

Communication service providers and governments should inform consumers of both the potential security and privacy challenges they may face when using communication networks and services and the available measures which can be used to limit these risks.

- *Communication service providers should implement data security policies and measures to prevent unauthorized transactions and data breaches.*
- *Security precautions and built-in security features should be developed.*

Annex C.
OECD POLICY GUIDANCE ON RADIO FREQUENCY IDENTIFICATION

Preface

The use of Radio Frequency Identification (RFID) technologies[1] is growing. Many different RFID applications are implemented in various sectors, and used for very different purposes. RFID is now at a stage where there are potentially large benefits from wider application but barriers remain, warranting a policy framework to enhance business and consumer benefits while effectively addressing security and privacy issues. From a public policy perspective, such a framework should be supportive, technology neutral encompassing all RFID technologies and provide the basis to protect citizens from current and future negative impacts of the technologies. These policy principles address barriers to wider application of RFID. They draw on policy discussions and analytical studies on RFID carried out by the OECD from 2005 to 2007.[2]

RFID enables wireless data collection by readers from electronic tags attached to or embedded in objects, for identification and other purposes. RFID systems involve software, network and database components that enable information to flow from tags to the organisation's information infrastructure where it is processed and stored. Systems are application-specific. Some use passive, low cost tags with short read ranges, most data on the network, and only small amounts of information on tags. Others use sophisticated, high performance tags with high data capacity or read ranges that can have considerable data on tags without network connection. At present, the higher capacity tags remain less commercially viable but their cost is decreasing and they are becoming part of wider, often sensor-based, systems.

RFID applications have been in use for many years in transport (public transport entry), access control cards (building and highway entry), event ticketing and management, and, more recently, in government identity cards and passports, and extensively in manufacturing supply chains and in logistics for goods distribution.

1. RFID may be considered as one of a group of automatic identification and data capturing technologies which also includes bar codes, biometrics, magnetic stripes, optical character recognition, smart cards, voice recognition and similar technologies.

2. See "Radio-Frequency Identification: a Focus on Security and Privacy" (2008) [DSTI/ICCP/REG(2007)9/FINAL], "Radio Frequency Identification Implementation in Germany: Challenges and Benefits" (2007) [DSTI/ICCP/IE(2007)6/FINAL], "Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations" (2006) [DSTI/ICCP(2005)19/FINAL], "Proceedings of the OECD Foresight Forum on Radio Frequency Identification Applications and Public Policy Considerations" (2005) [DSTI/ICCP(2006)7].

Industry sectors differ widely in RFID deployment, with many automotive companies and hospitals relying on RFID systems. Wholesale and retail businesses are rapidly adopting such systems, with a shift towards more comprehensive application strategies along sector value chains. Most tagging still occurs at the pallet and packing carton level, but there is a trend toward item-level tagging, beginning with high-value goods or components, as tag prices decline.

Business benefits are sector-specific and commonly include process optimisation, more efficient supply chain inventory management, and increased process quality and security including recycling and anti-counterfeiting applications. Most implementation projects are in their early stages and many businesses need to change the processes or their work organisation to better capture benefits. Broad societal benefits are expected from RFID in various areas ranging from food safety, product recall, drug identification, public health and medical applications, better warranty management, better, more detailed product information and improved stocking.

Technological developments are focusing on increasing real-time information of business processes, improved business performance and improved security and privacy. Combination with other technologies is important in the longer-term, and communications and sensor technologies will enable distance monitoring of ambient conditions (*e.g.* temperature, pressure) in applications such as healthcare and environment. Many of the technical challenges are imposed by the laws of physics, such as interference, power management, reflection, and signal attenuation.

Many of the potential societal challenges raised by RFID relate to its core characteristic: invisible electromagnetic communications that make the collection of information by RFID devices not obvious to the person carrying the tagged product or object. Tags' data depends on their use contexts. For example, in a supply chain/retail context, tags attached to products usually contain product-identifying information and privacy concerns arise after the point of sale; in credentials, tags sometimes contain personal information. The extent to which tags are traceable is determined by the read range of the combined tag and reader. Specific concerns include the controls of the tag reading, the protection of personal data, the ability to join trace information with other information to profile individuals and the use to which the information may be put. Longer-term concerns are related to the potential pervasiveness of tags and readers.

Like any other information technology, RFID systems are subject to security risks[3] affecting their integrity, availability and confidentiality such as denial of service, jamming, cloning, interception/eavesdropping, and unauthorised access to data ("skimming"). While not all uses of RFID implicate privacy concerns, RFID systems which collect or process information relating to identified or identifiable individuals are subject to privacy risks (*e.g.* unauthorised access to information stored in tags). The use of RFID in identity credentials, for example, poses heightened privacy concerns, and it is necessary to ensure privacy is appropriately protected. These risks, if not taken into account at an early stage, are likely to increase the costs of RFID applications and, more generally, impede the adoption of the technology and delay potential benefits.

3. *e.g.* cloning of speed-pass payment RFID cards and automobile ignition keys.

The OECD *Security Guidelines*[4] and *Privacy Guidelines*[5] provide a comprehensive framework for the security of information systems and network and the protection of privacy and personal data. This framework applies to RFID.

The policy principles that follow provide policy and practical guidance to enhance business and consumer benefits from the use of RFID while proactively taking into account security and privacy concerns. Principles 1 to 6 cover government and business policies and practices to increase the use of, and economic benefits from, wider applications of RFID and emerging related sensor applications. Government policy roles are directed at: incentives for R&D and generic technologies and applications; developing public sector applications and being model users; information, awareness and education activities, including in privacy and security areas and for small businesses; harmonisation of standards; and spectrum allocation issues. Principles 7 to 12 provide all stakeholders with guidance to support the implementation of the *Security and Privacy Guidelines* when they deploy RFID systems. Specific issues are addressed in relation to RFID systems or RFID components in broader systems, including the need for: a comprehensive approach to security and privacy management; security risk and privacy impact assessments; technical measures to protect security and privacy; individuals' information; and a general policy of transparency. Principle 13 calls for a continued dialogue among all stakeholders. Finally, the need for monitoring developments related to RFID is highlighted in Principle 14.

Principles

1. Support for R&D and new applications

Government support and incentives should focus on R&D for generic RFID-related technologies and applications.

Many of the technological areas underlying RFID are still being developed and there are wide economic benefits to be gained from continued research in areas critical to RFID development, including new materials, and new reading technologies that can be used at greater distances and that can overcome interference and operate in hostile environments. There are social benefits from continued research on issues related to RFID use in the healthcare or environmental areas, *e.g.* interference with other medical devices, impact of electromagnetic fields on individuals, or the effect tags will have on recycling practices. Further efforts to research and develop cost-effective technical measures embedding security and privacy protections in RFID systems should also be encouraged (see Principle 9).

4. *OECD Guidelines for the Security of Information Systems and Networks : Towards a Culture of Security* (2002).

5. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

2. Technological neutrality

Government policies to encourage the use and expand the benefits of RFID should be technology-neutral.

RFID technologies and applications are highly diverse and evolving rapidly. RFID technologies vary in terms of capabilities (*e.g.* frequency range, battery and memory capacity, size). Individual RFID applications involve a wide range of different operations and industry sectors. Attempts to focus support efforts on particular technologies or applications may diminish resources for other promising avenues and distort markets for components and equipments. Government policies to foster the use and expand the benefits of RFID should not favour one technology or application over another.

3. Governments as model users

As developers and users of RFID for public purposes, governments should share their experience and good practices as widely as possible.

Governments are developing innovative RFID applications in areas ranging from tracking art works and library and museum stocks to improved airport management and defence applications. Their experience and good practices in developing such applications can benefit other actors and should be shared as widely as possible to maximise the benefits from government investments and help diffusion of the technology.

4. Awareness and information

Governments should encourage initiatives to help raise awareness of the benefits and challenges of RFID and encourage sharing of information on large-scale pilots and demonstration projects.

Governments, in conjunction with business associations, the technical community and increasingly with consumer and other citizen groups, have experience in raising awareness of the benefits and challenges of emerging technology applications and their economic and social impacts. Clear and neutral information on RFID technologies, their characteristics and related security and privacy aspects can help small business and the general public appreciate the benefits and risks of these technologies and make informed choices in relation to their use. Governments should promote provision of such information at the earliest possible stage, particularly where applications have cross-sector implications and broad social impacts.

5. Standards

The development of consensus-based global standards for RFID should be encouraged. Issues such as standards convergence should be addressed through market mechanisms to the extent possible.

The development and use of RFID technical and management standards, within and across sectors, enables interoperability, encourages new market entry and allows for economies of scale in applications particularly at the international level. The development of open global RFID standards and standards harmonisation within and across sectors should involve all stakeholders. Standards can play an equally important role in facilitating security and privacy by design and good practices for RFID systems.

6. Spectrum

Governments should encourage and facilitate RFID applications when considering spectrum licensing and allocation.

Governments, manufacturers, standardisation bodies and other stakeholders should co-operate at international level to ensure interoperability, to consider harmonisation of frequency bands as appropriate, to limit harmful interference with other radio devices and users, and to ensure that devices operating within the specified frequency bands comply with the electrical power, radio standards and policy set for those systems, and encourage the development of internationally compatible applications. The exemption of licenses for frequency usage in RFID applications is a recognised licensing option, and is known to be a driver for RFID technology adoption.

7. Security and privacy management

Participants should adopt a comprehensive approach to developing a security and, where appropriate, a privacy management strategy which should be tailored to each RFID system and take into account the interests of all parties involved, including individuals.

All RFID systems require the development of a security management strategy which considers each stage of the system's life (planning, deployment, operation, data processing and end of life) and each component of the system (tags and readers, middleware, databases, network and back-end components).

Not all RFID systems require a privacy management strategy. Such strategy is required when an RFID system collects or processes information relating to an identified or identifiable individual. An organisation which implements an RFID system should conduct a careful analysis of whether the RFID information is personal data (*e.g.* name or personal identifier), or if the RFID information, while not personal data (*e.g.* object identifier), can be linked to an identified or identifiable individual (*e.g.* at the point of sale). In both cases, the RFID system requires a privacy management strategy which considers each step of the RFID data lifecycle, each stage of the system's life, and each component of the system.

8. Security risk and privacy impact assessments

Participants should conduct and periodically review a security risk assessment and, where appropriate, a privacy impact assessment.

Security risk assessment and, where applicable, privacy impact assessment are essential tools for managing security and privacy in relation to RFID systems. Such assessments are necessary to determine the appropriate preventative and mitigation measures to manage the risk of potential harm to RFID systems, to the organisation, and to individuals in light of the nature and sensitivity of the information to be protected. Security risk assessments and privacy impact assessments should take into consideration the technology, the application and operational scenarios, and consider the entire life cycle of the actual RFID tags including those that remain functional even when no longer under the control of the organisation.

The privacy impact assessment of an RFID system should consider whether it is necessary to collect and process information relating to an identified or identifiable individual. It should also take into account the possibility of linking data collected or transmitted using RFID with other data and the potential impact those linkages could have on individuals. This becomes even more important in the case of sensitive personal data (*e.g.* biometric, health, or identity credential data), as does the issue of protecting the data. Finally, organisations could consider making their privacy impact assessments public, as appropriate.

9. Technical measures to protect security and privacy

Participants who develop or operate RFID technologies and systems should adopt technical security and privacy protection measures in the design and operation of their systems.

A combination of technical and non-technical safeguards is required to ensure security and protect privacy in relation to RFID technologies and systems. Cost-effective technical measures embedding security and privacy protections can play a significant role in reducing risks related to, and fostering trust in, RFID technologies and systems. A number of measures are either available or under development (*e.g.* deactivation, authentication mechanisms, cryptography, data minimisation and anonymisation). Further efforts towards their adoption should be encouraged.

10. Knowledge and consent

Participants who collect or process information relating to identified or identifiable individuals using RFID should do so with the knowledge and, where appropriate, the consent of the individuals concerned.

Individuals should be informed about, or, where appropriate, have the possibility to consent to, the collection, processing, storage and dissemination of RFID data relating to them. Their knowledge or consent should be based on an understanding of the entire RFID data life cycle not just the initial transmission. Governments should encourage all participants to work towards a consensus on the circumstances under which consent should or should not be required.

11. Privacy notices

Participants who collect or process information relating to identified or identifiable individuals using RFID could include more information in RFID privacy notices than in usual privacy notices, given the invisibility of the data collection.

In addition to information about the data collected, the purpose of the collection and the right of access, privacy notices could include all or part of the following: *i)* the existence of tags, *ii)* their content, use and control, *iii)* the presence of active readers, *iv)* the ability to disable tags and *v)* where to obtain assistance. Such explanatory information would also help educate the public about the new technology. Research towards innovative notification practices, standardised notices and technical means to improve user notification should be encouraged.

12. Transparency

Participants who provide functional tags to individuals — whether or not they collect personal data — should inform individuals about the existence of the tags, any associated privacy risks, and any measures to mitigate these risks.

Participants who provide individuals with RFID tags that remain functional and could be read at a later stage, including by third parties, should have a general policy of transparency about the existence of such tags, their content, any potential privacy risks in presence of active readers, any measures to prevent or mitigate risks such as information on how to deactivate the tags, information on where to obtain assistance, and any further relevant information. Furthermore, there should be a possibility for individuals to disable RFID tags transparently, easily and without extra cost. It is however recognised that there may be specific circumstances in which it would be impossible or involve disproportionate efforts to provide such information, or in which it would not be in the individuals' best interest to disable the RFID devices.

13. Continued dialogue

Governments should encourage all participants to continue to work towards better policies to enhance the economic and social benefits from wider applications of RFID and effectively address outstanding security and privacy issues.

A continued dialogue between all participants will enhance the economic and social benefits from wider applications of RFID, and foster increased security and privacy in RFID systems. The usefulness of such dialogue has already been mentioned in areas such as awareness and information, standards, spectrum, individuals' knowledge and consent, and transparency. Extending the dialogue to the development, publication and adoption of good practices more widely, including security and privacy practices, would facilitate wider diffusion of RFID technologies and help address concerns raised by their potential widespread adoption.

14. Looking forward: monitoring evolution

Governments should encourage research and analysis on the economic and social impacts of the use of RFID in conjunction with other technologies and systems.

Because of continuous technical innovation and its impact on the economy and society, monitoring developments and detecting trends early is essential to identify new opportunities to be seized, new challenges to be addressed, and to adjust policies. Potential developments of RFID to be monitored include their combination with sensor-based systems, their cross-border use, the convergence of these technologies on the Internet, and their potential pervasiveness.

Annex D.
PRINCIPLES AND GUIDELINES FOR ACCESS TO RESEARCH DATA FROM PUBLIC FUNDING

I. Objectives

These *Principles and Guidelines for Access to Research Data from Public Funding* (hereafter the "*Principles and Guidelines*") provide broad policy recommendations to the governmental science policy and funding bodies of member countries on access to research data from public funding. They are intended to promote data access and sharing among researchers, research institutions, and national research agencies, while at the same time, recognising and taking into account, the various national laws, research policies and organisational structures of member countries.

The ultimate goal of these *Principles and Guidelines* is to improve the efficiency and effectiveness of the global science system. They are not intended to hinder its development with onerous obligations and regulations or impose new costs on national science systems.

II. Scope and definitions

These *Principles and Guidelines* are meant to apply to research data, whether already in existence or yet to be produced, that are supported by public funds for the purposes of developing publicly accessible scientific research and knowledge. The *Principles and Guidelines* are not intended to apply to research data gathered for the purpose of commercialisation of research outcomes, or to research data that are the property of a private sector entity. Access to such data is subject to a range of considerations that are beyond the scope of this document. Moreover, in some instances, access to or use of data may be restricted to safeguard the privacy of individuals, protect confidentiality, proprietary results or national security.

Research data

In the context of these *Principles and Guidelines*, "research data" are defined as factual records (numerical scores, textual records, images and sounds) used as primary sources for scientific research, and that are commonly accepted in the scientific community as necessary to validate research findings. A research data set constitutes a systematic, partial representation of the subject being investigated.

This term does not cover the following: laboratory notebooks, preliminary analyses, and drafts of scientific papers, plans for future research, peer reviews, or personal communications with colleagues or physical objects (*e.g.* laboratory

samples, strains of bacteria and test animals such as mice). Access to all of these products or outcomes of research is governed by different considerations than those dealt with here.

These *Principles and Guidelines* are principally aimed at research data in digital, computer-readable format. It is indeed in this format that the greatest potential lies for improvements in the efficient distribution of data and their application to research because the marginal costs of transmitting data through the Internet are close to zero. These *Principles and Guidelines* could also apply to analogue research data in situations where the marginal costs of giving access to such data can be kept reasonably low.

Research data from public funding

Research data from public funding is defined as the research data obtained from research conducted by government agencies or departments, or conducted using public funds provided by any level of government. Given that the nature of "public funding" of research varies significantly from one country to the next, these *Principles and Guidelines* recognise that such differences call for a flexible approach to improved access to research data.

Access arrangements

Access arrangements are defined as the regulatory, policy and procedural framework established by research institutions, research funding agencies and other partners involved, to determine the conditions of access to and use of research data.

III. Principles

A. Openness

Openness means access on equal terms for the international research community at the lowest possible cost, preferably at no more than the marginal cost of dissemination. Open access to research data from public funding should be easy, timely, user-friendly and preferably Internet-based.

B. Flexibility

Flexibility requires taking into account the rapid and often unpredictable changes in information technologies, the characteristics of each research field and the diversity of research systems, legal systems and cultures of each member country. Specific national, social, economic and regulatory implications should be considered when organisations develop research data access arrangements, and when governments develop policies to promote data access and review the implementation of these *Principles and Guidelines*.

C. Transparency

Information on research data and data-producing organisations, documentation on the data and specifications of conditions attached to the use of these data should be internationally available in a transparent way, ideally through the Internet. Lack of visibility of existing research data resources and future data collection poses serious obstacles to access.

Factors to consider in ensuring transparency include:

- Information on data-producing organisations and their holdings, documentation on available data sets and conditions of use should be easy to find on the Internet.
- Research organisations and government research agencies should actively disseminate information on research data policies to individual researchers, academic associations, universities and other stakeholders in the publicly funded research process.
- Whenever relevant, all members of the various research communities should assist in establishing agreements on standards for cataloguing data. The application of existing standards should be considered, whenever appropriate, in order to avoid placing additional burdens on research resources and work loads of researchers and their institutions.
- Information on data management and access conditions should be communicated among data archives and data producing institutions, so that best practices can be shared.

D. Legal conformity

Data access arrangements should respect the legal rights and legitimate interests of all stakeholders in the public research enterprise.

Access to, and use of, certain research data will necessarily be limited by various types of legal requirements, which may include restrictions for reasons of:

- National security: data pertaining to intelligence, military activities, or political decision making may be classified and therefore subject to restricted access.
- Privacy and confidentiality: data on human subjects and other personal data are subject to restricted access under national laws and policies to protect confidentiality and privacy. However, anonymisation or confidentiality procedures that ensure a satisfactory level of confidentiality should be considered by custodians of such data to preserve as much data utility as possible for researchers.
- Trade secrets and intellectual property rights: data on, or from, businesses or other parties that contain confidential information may not be accessible for research.
- Protection of rare, threatened or endangered species: in certain instances there may be legitimate reasons to restrict access to data on the location of biological resources for the sake of conservation.

- Legal process: data under consideration in legal actions (sub judice) may not be accessible.

Subscribing to professional codes of conduct may facilitate meeting legal requirements.

E. Protection of intellectual property

Data access arrangements should consider the applicability of copyright or of other intellectual property laws that may be relevant to publicly funded research databases. Factors to consider include:

- As public/private partnerships in the funding of research and related data production are increasing, balanced public/private arrangements should facilitate broad access to research data where appropriate. The fact that there is private sector involvement in the data collection should not, in itself, be used as a reason to restrict access to the data. Consideration should be given to measures that promote non-commercial access and use while protecting commercial interests, such as delayed or partial release of such data, or the voluntary adoption of licensing mechanisms. Such measures can allow the primary participants to fully exploit the research data without unnecessarily shutting off access.
- In those jurisdictions in which government research data and information are protected by intellectual property rights, the holders of these rights should nevertheless facilitate access to such data particularly for public research or other public-interest purposes.

F. Formal responsibility

Access arrangements should promote explicit, formal institutional practices, such as the development of rules and regulations, regarding the responsibilities of the various parties involved in data-related activities. These practices should pertain to authorship, producer credits, ownership, dissemination, usage restrictions, financial arrangements, ethical rules, licensing terms, liability, and sustainable archiving.

Access arrangements, whether at the governmental or institutional levels, should be developed in consultation with representatives of all directly affected parties. In collaborative research programmes or projects, and especially in international scientific co-operation or in research projects based on public/private partnerships where there are differences in regulatory frameworks, the parties involved should negotiate research data sharing arrangements as early as possible in the life of the research project, ideally at the initial proposal stage. This will help ensure that adequate and timely consideration will be given to issues such as the allocation of resources for sharing and sustainable preservation of research data, differences in national intellectual property laws, limitations due to national security, and the protection of privacy and confidentiality.

Access arrangements also should be responsive to factors such as the characteristics of the data, their potential value for research purposes, the level of data processing (raw versus partially processed versus final), whether they are

homogeneous data from a facility instrument or sensor versus heterogeneous field data collected by single researchers, data on human subjects or physical parameters, and whether the data are generated directly by a government entity or as a result of government funding. These variations in the origin or type of data should be taken into consideration when establishing data access arrangements.

Further, consideration should be given to the following:

- Many of the problems related to access, dissemination and sharing of data result from the lack of explicit institutional agreements on the terms of access and use. With data management becoming ever more complex in certain areas of research, traditional informal arrangements between researchers may no longer be adequate and may need to be complemented by formally agreed practices and procedures.
- Responsibility for the various aspects of data access and management should be established in relevant documents, such as descriptions of the formal tasks of institutions, grant applications, research contracts, publication agreements, and licenses.
- Long-term sustainability of the infrastructure required for data access is particularly important. Research institutions and government organisations should take formal responsibility for ensuring that research data are effectively preserved, managed and made accessible in order that they can be put to efficient and appropriate use over the long term.

G. Professionalism

Institutional arrangements for the management of research data should be based on the relevant professional standards and values embodied in the codes of conduct of the scientific communities involved.

Factors to consider include:

- The use of codes of conduct for professional scientists and their communities could help simplify and reduce the regulatory burden placed on access.
- Mutual trust between researchers, and trust between researchers, their institutions and other organisations plays an important role in the establishment and maintenance of such codes of conduct.
- In current research practice, the initial data-producing researcher or institution is sometimes rewarded with temporary exclusive use of the data. The rules for such incentive arrangements should be developed and explicitly stated by the funding sources in co-operation with the affected research communities.

In certain areas of science, a lack of planning for and execution of the proper documentation and archiving of data sets is one of the key impediments to realising maximum value from the investment in research data. Project and program planning activities, at all levels, should expressly acknowledge data issues at the earliest stages to take into consideration funding and technical assistance for the essential organisation and curation of those data sets. Attention should be paid to incentives

and the development of professional expertise in all areas of research data management.

H. Interoperability

Technological and semantic interoperability is a key consideration in enabling and promoting international and interdisciplinary access to and use of research data. Access arrangements, should pay due attention to the relevant international data documentation standards. member countries and research institutions should co-operate with international organisations charged with developing new standards.

Although science is becoming a highly globalised endeavour, incompatibility of technical and procedural standards can be the most serious barrier to multiple uses of data sets.

Factors that should be considered include:

- The standards employed should be explicitly mentioned as this is the first requirement for interoperability.
- Adoption of the practices of disciplines most advanced in this respect should be promoted, in particular by the international professional organisations dealing with science and the collection and preservation of data for research and technological purposes.
- The work of organisations engaged in setting more general information and communication technology standards should also be considered.

I. Quality

The value and utility of research data depends, to a large extent, on the quality of the data itself. Data managers, and data collection organisations, should pay particular attention to ensuring compliance with explicit quality standards. Where such standards do not yet exist, institutions and research associations should engage with their research community on their development. Although all areas of research can benefit from improved data quality, some require much more stringent standards than others. For this reason alone, universal data quality standards are not practical. Standards should be developed in consultation with researchers to ensure that the level of quality and precision meets the needs of the various disciplines.

More specifically,

- Data access arrangements should describe good practices for methods, techniques and instruments employed in the collection, dissemination and accessible archiving of data to enable quality control by peer review and other means of safeguarding quality and authenticity.
- The origin of sources should be documented and specified in a verifiable way. Such documentation should be readily available to all who intend to use the data and incorporated into the metadata accompanying the data sets. Developing such metadata is important for enabling scientists to understand the exact implications of the data sets.

- Whenever possible, access to data sets should be linked with access to the original research materials, and copied data sets should be linked with originals, as this facilitates validation of the data and identification of errors within data sets.
- Research institutions and professional associations should develop appropriate practices with respect to the citations of data and the recording of citations in indexes, as these are important indicators of data quality.

J. Security

Specific attention should be devoted to supporting the use of techniques and instruments to guarantee the integrity and security of research data. With regard to guaranteeing the integrity of a data set, every effort should be made to ensure the completeness of data and absence of errors. With regard to security, the data, along with relevant meta-data and descriptions, should be protected against intentional or unintentional loss, destruction, modification and unauthorised access in conformity with explicit security protocols. Data sets and the equipment on which they are stored should be protected as well from environmental hazards such as heat, dust, electrical surges, magnetism, and electrostatic discharges.

K. Efficiency

One of the central goals of promoting data access and sharing is to improve the overall efficiency of publicly funded scientific research to avoid the expensive and unnecessary duplication of data collection efforts.

Consideration should be given to the following:

- Data access arrangements should promote further cost effectiveness within the global science system by describing good practices in data management and specialised support services.
- While publicly funded research data are subject to the default rule of openness under Principle A, this does not mean that all such data should be preserved permanently. The data archiving community should carry out cost-benefit assessments periodically and constantly develop and refine retention protocols to ensure that those data sets with the greatest potential utility are preserved and made accessible. Use of accepted retention protocols and thorough documentation of data should help to reduce unnecessary duplication of effort as well as to establish the necessary selectivity in preservation.
- Specialised support services, for example through collaboration with non-academic specialists on specific research projects or the engagement of data management specialist organisations, should be considered as a means to ensure the cost-effective production, use, management and archiving of research data.
- Insufficient incentives for researchers or database producers may lessen their efforts on data-related activities. The development of new reward structures and the adaptation of existing ones, including recognition of data

management activities in tenure and promotion review, should be considered as a way to address this problem.

L. Accountability

The performance of data access arrangements should be subject to periodic evaluation by user groups, responsible institutions and research funding agencies. Although each party is likely to use somewhat different evaluation criteria, the sum total of the results should provide a comprehensive picture of the value of data and of data access regimes. Such evaluations should help to increase the support for open access among the scientific community and society at large.

The following should be considered in establishing evaluation criteria:

- Overall public investments in the production and management of research data.
- Management performance of data collection and archival agencies.
- Extent of re-use of existing data sets.
- Knowledge generated from the re-use of existing data.
- The use of targeted foresight exercises to determine the nature and scope of data preservation activities and the types of data most likely to be needed in the future.

Even if gaining clear insight into the cost, benefit and performance of data access arrangements will not be an easy task, those in charge of data access arrangements should put effort into showing the benefits of open data access to justify and help ensure sustained support from all levels of government.

M. Sustainability

Due consideration should be given to the sustainability of access to publicly funded research data as a key element of the research infrastructure. This means taking administrative responsibility for the measures to guarantee permanent access to data that have been determined to require long-term retention. This can be a difficult task, given that most research projects, and the public funding provided, have a limited duration, whereas ensuring access to the data produced is a long-term undertaking. Research funding agencies and research institutions, therefore, should consider the long-term preservation of data at the outset of each new project, and in particular, determine the most appropriate archival facilities for the data.

Annex E.
OECD POLICY GUIDANCE FOR DIGITAL CONTENT

Digital content has become an increasingly important and pervasive factor shaping economic and social development. High-speed communications, increasing upstream as well as downstream bandwidth, declining access prices, convergence of previously distinct networks, innovation in new devices and applications and lower entry barriers will drive new ways of creating, distributing, preserving, and accessing digital content. As economies move towards being more knowledge-intensive, information-rich activities in which content is created, collected, managed, processed, stored, delivered, and accessed are spreading into a broad range of industries, contributing to further innovation, growth and employment. Digital content is becoming central in research, health, education and social services, knowledge and cultural services and government. It is also stimulating increased participation and creative supply by users.

Appropriate policies can increase the contribution of digital content to growth and welfare and spread the benefits more widely. The 2004 OECD Recommendation of the Council on Broadband Development[1] recognised the growing role of digital content and the Working Party on the Information Economy has undertaken extensive analysis of digital broadband content developments and strategies and associated policies.[2] These principles build on this work, the conference on 'The Future Digital Economy: Digital Content Creation, Distribution and Access' and on national inputs.

The objective of these principles is to help provide and inform the context for policy discussion, policy analysis, review and development. Further work will be undertaken by the OECD and its member countries to both implement this framework, and review and improve it in the future.[3] A range of stakeholders have interests in these issues. It is important to recognise and involve them in further

1. See the report *Monitoring the Recommendation of the Council on Broadband Development*, C(2008)51.

2. See analytical studies at www.oecd.org/sti/digitalcontent. These studies use a common methodological approach to deal with emerging challenges and policy issues. They comprise: scientific publishing, music, online computer and video games, mobile content, public sector information, user-created content, film and video and online advertising, An analysis of strategies and policies is contained in OECD (2006), *Digital broadband content: Digital content strategies and policies*, DSTI/ICCP/IE(2005)3/FINAL.

3. Further work is also needed in measuring digital content, developing appropriate international indicators and metrics, and improving systematic and comparable data collection, research and analysis.

work to ensure that the benefits of digital content-related innovations and the wide diffusion of content, information, and knowledge are achieved.

Governments and digital content

It is clearly recognised that market participants create and develop digital content business models but governments have a role in developing "enabling factors" for creation and use of digital content, taking measures to support cultural diversity and local content-related entrepreneurship, and acting as facilitators by enhancing capabilities and removing unnecessary regulatory barriers and other impediments across previously separate policy areas. Elimination of barriers to competition in network services, and policies that promote investment in broadband infrastructure, content and capabilities in rural and remote regions and developing economies play an important role. An appropriate 'pro-digital content' business environment can be developed by addressing market failures that hamper R&D, innovation, education and skill development. Non-discriminatory framework conditions can reduce barriers to entry, improve competitive conditions and help overcome lack of finance. Governments also have a major role as creators and users of digital content.[4]

Digital content principles[5]

The following policy principles will help promote an enabling environment, enhance the infrastructure, and foster a business and regulatory climate conducive to the creation, access to and preservation of digital content.

Promoting an enabling environment

- Policies that encourage a creative environment that stimulates market and non-market digital content creation, dissemination, and preservation of all kinds.
- Policies that facilitate R&D and innovation in digital content creation, dissemination, and preservation, and digital content-related networks, software and hardware, open standards, and interoperability.
- Policies that help ensure that capital markets (*e.g.* venture and risk capital) work competitively in funding innovation and digital content ventures.
- Initiatives aimed at addressing shortages in skills, training, education and human resource development for the creation, distribution and use of innovative digital content.

4. See separate *Recommendation of the Council for enhanced access and more effective use of public sector information* C(2008)36.

5. For consistency the terms "digital content creation, dissemination, and preservation" and "use," have been used as appropriate in the text unless a particular situation requires the use of a specific term.

- Policies that stimulate enhanced knowledge creation, dissemination, lawful use and preservation of different forms of digital content, (including access to information, research, data and publications), encourage investments in such creation, dissemination and preservation, and encourage global access to content regardless of language and origin.
- Policies that enhance access and more effective use of public sector information.
- Creating and ensuring an environment that promotes freedom of expression and access to information and ideas.

Enhancing the infrastructure

- Policies that encourage investment in new network infrastructure, software, content and applications.
- Policies that work to improve regulatory parity and consistent policy treatment across different, and in some cases converging, content delivery platforms (including next-generation networks), technological environments and value chains.
- Policies that encourage technology neutral approaches, interoperability and open standards development to address technological issues related to digital content creation, dissemination, use and preservation.
- Policies that improve applications for the delivery and use of digital content, including promoting effective management, preservation and dissemination tools that enhance access and use of different types of digital content.
- Policies that promote and enhance accessibility to digital content of all people regardless of location in order to realise the full benefits of the Internet economy and the global digital environment.

Fostering the business and regulatory climate

- Policies that encourage the development of innovative business models, the spread of best practices and the adaptation of value chains in the digital environment.
- Policies supporting non-discriminatory business and policy frameworks that reinforce competition.
- Policies that recognise the rights and interests of creators and users, in areas such as the protection of intellectual property rights, while encouraging innovative e-business models.
- Policies that provide incentives for the creation, dissemination, and preservation of digital content (*e.g.* through open innovation strategies, university-business collaboration, providing incentives for long-term research, and through intellectual property rights).

- Policies to improve information and content quality and accuracy; for example, policies that facilitate the use of tools to help creators identify and disseminate their works and users to identify and access specific information and works.
- Policies that enhance confidence in the creation and use of digital content through effective enforcement of privacy and consumer protection, by discouraging identity misrepresentation and theft and protecting children from harmful content by clearly informing users of means of protection, by reducing digital copyright infringement, by promoting information and network security while striking the balance between openness and security in content environments, and more generally by strengthening cross-border co-operation and practical measures to reach these goals.
- Policies that improve online commercial transactions including mechanisms for payment and micro-payments, electronic signatures and authentication, and international interoperability of these mechanisms.
- Clarifying taxation issues as they relate to digital content products.

Annex F.
OECD RECOMMENDATION OF THE COUNCIL FOR ENHANCED ACCESS AND MORE EFFECTIVE USE OF PUBLIC SECTOR INFORMATION

THE COUNCIL

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Access to Research Data from Public Funding [C(2006)184] and the Recommendation of the Council on Broadband Development [C(2003)259];

Having regard to the aim to increase returns on public investments in public sector information1 and increase economic and social benefits from better access and wider use and re-use,2 in particular through more efficient distribution, enhanced innovation and development of new uses;

Having regard to the aim to promote more efficient distribution of information and content as well as the development of new information products and services particularly through market-based competition among re-users of information;

Considering the usefulness of collectively agreed principles for enhanced access and more effective use and re-use of public sector information for both the public and the private sector;

Recognising that efforts to improve the access and use of public sector information need to take into account legal requirements and restrictions, including intellectual property rights and trade secrets, effective and secure management of personal information, confidentiality and national security concerns, and fundamental principles including democracy, human rights and freedom of information and that, consequently, certain principles contained in this Recommendation regarding in particular openness and re-use, can be applied to a different extent to different categories of public sector information;

1. "Public sector information" is broadly defined for purposes of this Recommendation as "information, including information products and services, generated, created, collected, processed, preserved, maintained, disseminated, or funded by or for the Government or public institution", taking into account the legal requirements and restrictions referred to in the last paragraph of the preamble of this Recommendation.

2. This includes use by the original public sector generator or holder or other public sector bodies and further re-use by business or individuals for commercial or non-commercial purposes. In general, the term "use" implies this broad spectrum of use and re-use.

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS that, in establishing or reviewing their policies regarding access and use of public sector information, Member countries take due account of and implement the following principles, which provide a general framework for the wider and more effective use of public sector information and content and the generation of new uses from it:

- **Openness.** Maximising the availability of public sector information for use and re-use based upon presumption of openness as the default rule to facilitate access and re-use. Developing a regime of access principles or assuming openness in public sector information as a default rule wherever possible no matter what the model of funding is for the development and maintenance of the information. Defining grounds of refusal or limitations, such as for protection of national security interests, personal privacy, preservation of private interests for example where protected by copyright, or the application of national access legislation and rules.

- **Access and transparent conditions for re-use.** Encouraging broad non-discriminatory competitive access and conditions for re-use of public sector information, eliminating exclusive arrangements, and removing unnecessary restrictions on the ways in which it can be accessed, used, re-used, combined or shared, so that in principle all accessible information would be open to re-use by all. Improving access to information over the Internet and in electronic form. Making available and developing automated on-line licensing systems covering re-use in those cases where licensing is applied, taking into account the copyright principle below.

- **Asset lists.** Strengthening awareness of what public sector information is available for access and re-use. This could take the form of information asset lists and inventories, preferably published on-line, as well as clear presentation of conditions to access and re-use at access points to the information.

- **Quality.** Ensuring methodical data collection and curation practices to enhance quality and reliability including through cooperation of various government bodies involved in the creation, collection, processing, storing and distribution of public sector information.

- **Integrity.** Maximising the integrity and availability of information through the use of best practices in information management. Developing and implementing appropriate safeguards to protect information from unauthorised modification or from intentional or unintentional denial of authorised access to information.

- **New technologies and long-term preservation.** Improving interoperable archiving, search and retrieval technologies and related research including research on improving access and availability of public sector information in multiple languages, and ensuring development of the necessary related skills. Addressing technological obsolescence and challenges of long term preservation and access. Finding new ways for the digitisation of existing public sector information and content, the development of born-digital public sector

information products and data, and the implementation of cultural digitisation projects (public broadcasters, digital libraries, museums, etc.) where market mechanisms do not foster effective digitisation.

- **Copyright.** Intellectual property rights should be respected. There is a wide range of ways to deal with copyrights on public sector information, ranging from governments or private entities holding copyrights, to public sector information being copyright-free. Exercising copyright in ways that facilitate re-use (including waiving copyright and creating mechanisms that facilitate waiving of copyright where copyright owners are willing and able to do so, and developing mechanisms to deal with orphan works), and where copyright holders are in agreement, developing simple mechanisms to encourage wider access and use (including simple and effective licensing arrangements), and encouraging institutions and government agencies that fund works from outside sources to find ways to make these works widely accessible to the public.
- **Pricing.** When public sector information is not provided free of charge, pricing public sector information transparently and consistently within and, as far as possible, across different public sector organisations so that it facilitates access and re-use and ensures competition. Where possible, costs charged to any user should not exceed marginal costs of maintenance and distribution, and in special cases extra costs for example of digitisation. Basing any higher pricing on clearly expressed policy grounds.
- **Competition.** Ensuring that pricing strategies take into account considerations of unfair competition in situations where both public and business users provide value added services. Pursuing competitive neutrality, equality and timeliness of access where there is potential for cross-subsidisation from other government monopoly activities or reduced charges on government activities. Requiring public bodies to treat their own downstream/value-added activities on the same basis as their competitors for comparable purposes, including pricing. Particular attention should be paid to single sources of information resources. Promoting non-exclusive arrangements for disseminating information so that public sector information is open to all possible users and re-users on non-exclusive terms.
- **Redress mechanisms.** Providing appropriate transparent complaints and appeals processes.
- **Public-private partnerships.** Facilitating public-private partnerships where appropriate and feasible in making public sector information available, for example by finding creative ways to finance the costs of digitisation, while increasing access and re-use rights of third parties.
- **International access and use.** Seeking greater consistency in access regimes and administration to facilitate cross-border use and implementing other measures to improve cross-border interoperability, including in situations where there have been restrictions on non-public users. Supporting international co-operation and co-ordination for commercial re-use and non-commercial use. Avoiding fragmentation and promote greater interoperability and facilitate sharing and comparisons of national and inter-

national datasets. Striving for interoperability and compatible and widely used common formats.

- **Best practices.** Encouraging the wide sharing of best practices and exchange of information on enhanced implementation, educating users and re-users, building institutional capacity and practical measures for promoting re-use, cost and pricing models, copyright handling, monitoring performance and compliance, and their wider impacts on innovation, entrepreneurship, economic growth and social effects.

INVITES:

Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps to enhance access and promote more effective use of public sector information;

Non-member economies to take account of this Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the OECD Committee for Information, Computer and Communications Policy to promote the implementation of this Recommendation and review it every three years to foster enhanced access and more effective use of public sector information.

Annex G.
OECD RECOMMENDATION OF THE COUNCIL ON THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES

THE COUNCIL

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131], hereinafter the "Security Guidelines";

Having regard to the Resolution 58/199 adopted by the General Assembly of the United Nations on the creation of a global culture of cybersecurity and the protection of critical information infrastructures;

Recognising that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and inter-dependent, domestically and across borders; that a number of those systems and networks are of national critical importance; and that their protection is a priority area for national policy and international cooperation;

Recognising that in order to improve the protection of domestic and cross-border critical information infrastructures, Member countries need to share their knowledge and experience in developing policies and practices and cooperate more closely between themselves as well as with non Member economies;

Recognising that the protection of critical information infrastructures requires coordination domestically and across borders with the private sector owners and operators of such infrastructures, hereinafter the “private sector”;

On the proposal of the Committee for Information, Computer and Communication Policy:

AGREES that:

For the purposes of this Recommendation, critical information infrastructures, hereinafter “CII”, should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy;

National CII are identified through a risk assessment process and typically include one or more of the following:

- Information components supporting critical infrastructures, and/or
- Information infrastructures supporting essential components of government business; and/or
- Information infrastructures essential to the national economy.

RECOMMENDS that:

Member countries introduce and maintain an effective framework to implement the OECD Security Guidelines in relation to the protection of CII, taking into account the specific policy and operational guidance set out herein;

PART I. Protection of critical information infrastructures at the domestic level

Member countries should:

Demonstrate government leadership and commitment to protect CII by:

- Adopting clear policy objectives at the highest level of government.
- Identifying government agencies and organisations with responsibility and authority to implement these policy objectives.
- Consulting with private sector owners and operators of CII to establish mutual cooperation for the implementation of these objectives.
- Ensuring transparency on the delegations of responsibility to government authorities and agencies to facilitate closer co-operation within the government and with the private sector.
- Systematically reviewing policy and legal frameworks and self-regulatory schemes which may apply to CII, including those addressing cross-border threats, to assess the need to enhance their implementation, to amend them or to develop new instruments.
- Taking steps, where appropriate, to enhance the security level of components of information system and networks that constitute CII.

Manage risks to CII by:

- Developing a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector.
- Taking into consideration interdependencies.
- Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern.
- Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:

i) The appropriate organisational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure preparedness, including prevention, protection, response and recovery from natural and malicious threats.

ii) A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.

- Developing an incident response capability, such as a computer security incident response team (CERT/CSIRTs), in charge of monitoring, warning, alerting and carrying out recovery measures for CII; and mechanisms to foster closer cooperation and communications among those involved in incident response.

Work in partnership with the private sector by:

- Establishing trusted public-private partnerships with a focus on risk management, incident response and recovery.
- Enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.
- Fostering innovation through public-private research and development projects focused on the improvement of the security of CII and as appropriate, sharing these innovations across borders.

PART II. Protecting critical information infrastructures across borders

Member countries should cooperate among themselves and with the private sector at the strategy, policy and operational levels to ensure the protection of CII against events and circumstances beyond the capacity of individual countries to address alone.

They should in particular proactively engage in bilateral and multilateral co-operation at regional and global levels with a view to:

- Share knowledge and experience with respect to the development of domestic policies and practices and to models for coordinating with private sector owners and operators of critical information infrastructures.
- Develop a common understanding of:

i) Risk management applicable to cross-border dependencies and inter-dependencies.

ii) Generic vulnerabilities, threats and impacts on the CII, to facilitate collective action to address those that are widespread, such as security flaws and malicious software, as well as to improve risk management strategies and policies.

- Make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action.

- Acknowledge the value of participation in international or regional networks for watch, warning and incident response, to enable robust information sharing and coordination at the operational level, as well as to better manage crisis in case of an incident developing across borders.
- Support cross-border collaboration for, and information sharing on, public-private research and development for the protection of CII.

INVITES:

Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps for the protection of CII;

Non-Member economies to take account of this Recommendation and collaborate with Member countries in its implementation;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to:

Promote the implementation of this Recommendation and review it every five years to foster international co-operation on issues relating to the protection of CII.

Annex H.
OECD POLICY GUIDANCE ON ONLINE IDENTITY THEFT

I. Introduction

Identity theft ("ID theft") is a longstanding problem which, as the Internet and E-commerce have developed, has expanded to include online forms. While the scope of online ID theft appears to be limited in most countries, its implications are significant as the growing risk of such theft can undermine consumer confidence in using the Internet for E-commerce. Governments have acted to fight against such fraud (both online and offline) at the domestic and international levels. The *1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("the 1999 Guidelines") and the *2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* ("the 2003 Guidelines"), for example, set out principles aimed at strengthening member countries' frameworks to fight offline and online fraud. Outside the OECD, international instruments such as the Council of Europe's *Cybercrime Convention* and the United Nations' *Convention against Transnational Organised Crime* have been developed to address the issue (see Appendix H.1).

The principles in the 1999 and 2003 *Guidelines* serve as a solid basis for establishing a framework to fight online ID theft and other fraud. The purpose of this paper is to describe how the principles presented in these instruments could be elaborated to strengthen and develop effective member country strategies to combat online ID theft. It explores, in particular, how education and awareness of stakeholders could be enhanced to prevent such theft. The guidance draws largely on the research and analysis contained in a *Scoping Paper on Online Identity Theft* that was considered by the Committee on Consumer Policy in 2007 (OECD, 2008).

ID theft definition, forms and methods

ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes. Although this definition encompasses both individuals and legal entities, focus in the present guidance is limited to identity theft affecting consumers.

Traditionally, ID theft has been committed by accessing information acquired from public records, theft of personal belongings, improper use of databases, credit cards, and checking and saving accounts and misusing that information. As described in Box 1 below, off-line, unauthorised access to personal data can be carried out by various means, including dumpster diving, payment card theft, pretexting, shoulder surfing, skimming, or business record theft.

Box 1. Traditional ways to access personal data for ID theft

Dumpster diving. Generally refers to the act whereby fraudsters go through bins to collect "trash" or discarded items. It is the means that identity thieves employ to obtain copies of individuals' cheques, credit card or bank statements, or other records that contain their personal information.

Pretexting. Pretexters are parties who contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished by an insider at the financial institution, or by fraudulently opening an online account in a customer's name.

Shoulder surfing. Refers to the act of looking over someone's shoulder or from a nearby location as the victim enters a personal identification number ("PIN") at an ATM machine.

Skimming. The capturing of personal data from the magnetic stripes on the backs of credit cards; data is then transmitted to another location where it is re-encoded onto fraudulently made credit cards.

Business record theft. Refers to situations where someone steals data from a business (*e.g.* stolen computers or files) or bribes insiders to obtain the information from the business or organisation.

On line, there are principally three methods to obtain victims' personal information (see Box 2): *i*) software designed to collect personal information is secretly installed on someone's computer or device – fixed or mobile (*i.e*. malware); *ii*) deceptive e-mails or websites are used to trick persons into disclosing personal information (*i.e*. phishing – phishing e-mails are often mass-distributed via spam; they are increasingly used to install malware on the computers of recipients.); and *iii*) computers or mobile devices are hacked into or otherwise exploited to obtain personal data.

Box 2. Online methods for stealing personal information

Malware. A general term for a software code or programme inserted into an information system in order to cause harm to that system or to other systems, or to subvert them for use other than that intended by their own users. Viruses, worms, Trojan horses, backdoors, keystroke loggers, screen scrapers, rootkits, and spyware are all examples of malware (See Appendix H.3 for definitions of these terms).

Spam. Commonly understood to mean unsolicited, unwanted and harmful electronic messages (OECD, 2006c) and is increasingly being viewed as a vector for malware and criminal phishing scams.

Phishing. A method that thieves use to lure unsuspecting Internet users' personal identifying information through emails and mirror-websites which look like those coming from legitimate businesses, such as financial institutions or government agencies. Typically, a phishing attack is composed of the following steps:

- The phisher sends its potential victim an e-mail that appears to be from an existing company. The e-mail uses the colours, graphics, logos and wording of the company.
- The potential victim reads the e-mail and provides the phisher with personal information by either responding to the e-mail or clicking on a link and providing the information via a form on a website that appears to be from the company in question.
- Through this, the victim's personal information is directly transmitted to the scammer.

Hacking. Exploiting vulnerabilities in electronic systems or computer software to steal personal data.

Prevalence

ID theft is an increasing problem victimising individuals across all ages and social categories. Box 3 describes the ways that identity thieves misuse consumers' personal information both off line and on line. Online ID theft has been recognised as the source of growing concerns for consumers in recent years, having a direct impact on E-commerce transactions, including mobile commerce (OECD, 2006c, p. 21). As noted in the *EU 2006 Special Eurobarometer* (European Commission, 2006, p. 12), the use of the Internet to purchase goods and services online is rather limited (only 27% of the EU population in 2005), and is mostly restricted to domestic commerce. Such limited use reflects, in part, consumers' lack of trust in E-commerce transactions, fearing that their personal information could be stolen.[1]

Box 3. Traditional and online methods of misusing personal information

Misuse of existing accounts. Identity thieves use victims' existing accounts, including credit card accounts, cheque/savings accounts, telephone accounts (both landline and wireless service), Internet payment accounts, E-mail and other Internet accounts, and medical insurance accounts.

Opening new accounts. Identity thieves use victims' personal information to open new accounts, including telephone accounts (both landline and wireless service), credit card accounts, loan accounts, cheque and savings accounts, Internet payment accounts, auto insurance accounts, and medical payment accounts.

Commit other frauds. Identity thieves also misuse victims' personal information by giving it to the police when stopped or charged with a crime, by using it to obtain medical treatment, services, or supplies, by using it in rental housing situations, by using it to obtain government benefits, and by using it in employment situations.

Efforts to combat ID theft

In recent years, a number of member countries have put programmes in place for addressing ID theft (see Appendix H.2). Such programmes, which tend to have strong educational and awareness aspects, target broad audiences including consumers, key employees from the public and private sector and law enforcement. An analysis of the challenges being faced suggests that efforts to combat online ID theft have three key aspects:

Prevention – what stakeholders can do to lower the risk of identities being stolen (*e.g*. ways to enhance identity security, ways to identify attempts and instances of identity theft, and ways to limit the magnitude and scope of incidents).

Deterrence – what stakeholders can do to discourage parties from engaging in ID theft (*e.g.* legal sanctions).

Recovery and redress – what stakeholders can do to facilitate recovery and redress of such harms as financial detriment, injury to reputation, and other non-monetary harms.

1. A 2006 *International Telecommunication Union Online Survey* (ITU, 2006) concluded that more than 40% of Internet users refrain from transacting on-line for that reason.

This guidance focuses on the prevention of the acquisition of personal information in the online environment. Section II provides ideas on how stakeholders can use education and enhanced awareness to *i*) help consumers avoid falling victim to ID theft and *ii*) help business and government fight more effectively against the problem. Section III deals specifically with initiatives that could be taken to educate business on ways to improve data security, while Section IV addresses issues related to identity authentication. Finally, Section V identifies areas where further work on ways to combat online ID theft would be beneficial. While the guidance is geared to online ID theft, it should be noted that many of the measures suggested are equally applicable to offline ID theft.

II. Ways that education and awareness could be enhanced to prevent online ID theft

Educating consumers, business, government officials, and the media, and raising awareness about online ID theft are indispensable to reducing risks of theft. Reducing these risks would strengthen consumer trust in E-commerce. As stated in the *1999 Guidelines*, "Governments, businesses and consumers representatives should work together to educate consumers about electronic commerce... to increase business and consumer awareness of the consumer protection framework that applies to their online activities" (OECD, 1999, Section VIII). This recommendation, which also appears in the *2003 Guidelines* (OECD, 2003, Section II. F), is directly relevant to online ID theft. Online ID theft is a fraudulent activity which has become increasingly complex, relying on ever changing high-tech methods. Tackling it requires concerted, collaborative efforts by all stakeholders (*i.e.* government, business, and consumers). Education and awareness are therefore necessary to ensure that both consumers and businesses are aware of the importance of the problem, and knowledgeable about its evolving forms.

Structuring education and awareness programmes

Effective education and awareness programmes require: *i*) development of compelling and informative educational materials; and *ii*) development of institutions and techniques to deliver the materials and education to stakeholders in efficient ways. Moreover, co-operation and co-ordination of initiatives among parties can provide important opportunities to exploit synergies and strengthen efforts. It is thus important to involve stakeholders at an early point in developing programmes; insights from different perspectives can help to better determine what the precise education/awareness needs are, what the target audiences might be, and how they could best be reached.

Collection of relevant information on online ID theft

The collection and dissemination of basic information on online ID theft are key to raising awareness and knowledge of the importance of the problem and ways to combat it. There are five basic types of information that it would be useful to develop: *i*) statistical information showing developments and trends; *ii*) information on the non-economic effects of ID theft; *iii*) factual material on the methods that parties are using to steal identities, *iv*) general tips on how to protect identity,

including tools that consumers and business could use to block online intrusions, and *v*) information on techniques that can be used to identify or recognise efforts to misuse identity information.

i) Statistical information showing developments and trends

In introducing and maintaining an effective framework to limit the incidence of fraudulent practices against consumers, the 2003 *Guidelines* call on member countries to provide for "effective mechanisms to adequately investigate, preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent ... practices" (OECD, 2003, Section II. A. 2). Awareness of the scope and scale of the problem is a key element in support of education campaigns. However, to date, information on developments and trends in online ID theft is not generally available, despite growing member country warnings that it is on the rise. Moreover, when data are available, they rarely include sufficient detail on online forms of ID theft (OECD, 2008).

It would be beneficial for stakeholders to explore ways to enhance the development of statistical information tracking developments in ID theft. It would be helpful if this information provided specific information on online ID theft. One of the indicators that has been used in this regard is the number of consumer complaints. It would be interesting to explore what other indicators may be helpful.

In addition to measuring the magnitude of ID theft, it could be useful to monitor its economic impact on individuals and countries. Such information would further highlight and illustrate the scale of the problem.

Information that is comparable from one country to another and from different sources within one country would enhance its value. The development of such information should, where possible, draw on the efforts of multilateral groups (both public and private) that are active in the area. Private-sector platforms could be used to gather, analyse and disseminate phishing, spam and virus statistics on a worldwide basis. These could include: the Anti-Phishing Working Group ("APWG," at www.antiphishing.org), which focuses on eliminating fraud and ID theft resulting from phishing and e-mail spoofing of all types; the Messaging Anti-Abuse Working Group ("MAAWG," at www.maawg.org), which aims at preserving the electronic messaging from online exploits and abuse such as messaging spam, malware attacks and other forms of abuse; and DigitalPhishNet ("DPN," www.digitalphishnet.org/default.aspx), which is a collaborative forum where Internet Service Providers, online auction sites, financial institutions, and law enforcement agencies share statistics and best practices in real time to tackle phishing and other online threats.

ii) Information on the indirect effects of ID theft

In addition to having economic costs, ID theft can have other effects including the time victims spend to restore their reputation, the negative effects on their reputation, and the subsequent difficulties they have to re-establish creditworthiness. Collection of such information would help provide a more complete understanding of the implications of ID theft, thereby helping to raise awareness of the problems that theft can cause.

iii) Factual material on the methods and techniques that parties are using to steal identities

Identifying the different techniques used to commit ID theft is crucial to effectively deterring and responding to the threat. To be useful, information on these techniques needs to be collected, analysed and updated on a regular basis to keep abreast of developments. Where possible, it would be beneficial to have such information processed and shared between and among not only consumer protection enforcement actors, but also other enforcement bodies addressing the ID theft issue. ID theft indeed raises, in many cases, security, privacy and spam issues (see Appendix H.1). Over the past years, ID thieves have shown a certain degree of ingenuity to get access to personal information. As indicated above, increasingly, malware and spam have been coupled with phishing.

As described in Box 4 below, phishing attacks have become ever more sophisticated, taking a variety of forms and targeting both fixed and mobile electronic devices.

Box 4. Phishing variants

Pharming: this method, which uses the same kind of spoofed identifiers as in a classic phishing attack, redirects users from an authentic website (*e.g.* a bank website) to a fraudulent site that replicates the original. When the customer connects its computer to its bank web server, a hostname lookup is performed to translate the bank's domain name (*e.g.* "bank.com") into an IP address. During that process, the IP address will be changed.

SmiShing: cell phone users receive text messages ("SMS") where a company confirms their signing up for one of its dating services and that they will be charged a certain amount per day unless they cancel their order at the company's website. Such a website is in fact compromised and used to steal personal information.

Vishing: in a classic spoofed e-mail, appearing from legitimate businesses or institutions, the phisher invites the recipient to call a telephone number. When calling, the target reaches an automated attendant, requesting personal data such as account number, or password for pretended "security verification" purposes. Victims feel usually safer in this way as they are not required to go to a website to transmit their personal information.

It should be noted that all stakeholders can play a role in developing and sharing information on the methods and techniques being employed. To maximise the utility of information that is collected, it is important that mechanisms be in place to facilitate the sharing of the information in an effective manner.

iv) Information on the level of sophistication of online ID techniques

In addition to understanding the process by which online ID theft can be committed, education campaigns need to warn consumers about the ever evolving forms of these methods. Phishing messages used to be quite unsophisticated and mostly text-based. For example, through the so-called "419 scam" (also well known as the online "Nigerian scam" or offline "Nigerian letter"), phishers tried to commit advance fee fraud by requesting upfront payment or money transfer from their targets. They usually offered to share a large amount of money with their potential victims that they would transfer out of their country. Victims were then asked to pay fees, charges or taxes to help release or transfer the money. However, victim of its

own success, this scam is today very well known among Internet users and is not used as much anymore.

Thus, understanding the need for more complex scams, phishers have developed new ways to trick consumers into revealing passwords, bank account numbers and other personal data. Phishing scams now increasingly contain well-designed images and logos copied from legitimate commercial institutions. They have also become more personalised, sometimes containing the first digits of their targets' credit card numbers - which may actually be found on all credit cards of the same bank – to further convince their potential victim that the message is coming from their own bank. Similar to real commercial offers, phishing scams contain multiple solicitations inviting targets to reveal the password, age, address, etc.

And while phishers traditionally used well-known top level domain names such as ".com", ".biz" or ".info", they now attempt to avoid detection by using domain names from small island countries, such as ".im" from the UK Isle of Man, which are in many cases unknown to spam filters (McAfee, 2006, p. 15). Some phishing scams now even contain self-signed digital certificates to use the "HTTPS" security protocol and trigger the security padlock icon on spoofed websites.

Keeping consumers and other stakeholders informed of new and evolving techniques is key to enhancing prevention.

v) General tips on how to protect identity while on line

Providing stakeholders with practical advice on ways to protect their identities (see Box 5) can contribute significantly to lowering the risk of, or preventing, online ID theft. A number of organisations and governments have developed tips in these areas. One of the most comprehensive and extensive initiatives was undertaken by the United States government, which maintains a website providing information on ways to protect personal information and avoid Internet fraud, including ID theft (http://onguardonline.gov/index.html).

Box 5. Consumer anti-phishing tips from OnGuardOnline.gov

- Install anti-virus and anti-spyware software, as well as a firewall on your fixed or mobile device and update them regularly.
- Avoid clicking on a link in a message that you think is spam and also make it a policy never to respond to e-mail or pop up messages that ask for your personal or financial information. Also, do not cut and paste a link from the message into your web browser. Phishers can make links look like they go one place, but then they actually take you to a look-alike site.
- Never disclose your credit card number or security digits in response to a message you suspect is spam. If you are concerned about your account, contact the organisation using a phone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself.
- Forward the phishing scam to law enforcers and/or to industry groups such as the APWG, DPN or MAAWG. You may also forward phishing e-mails to the FTC at spam@uce.gov. In addition to industry groups and law enforcement agencies, you may also forward the phishing e-mail to the organisation that is being spoofed.

Dissemination of information

Assuring that stakeholders are aware of, and have ready access to information on ID theft is key to enhancing prevention. At the very least, such information should be available on the Internet. In addition, orientation or training sessions in schools or on a group basis would be beneficial. Moreover, television and radio also provide opportunities to engage the public, as would the availability of printed or electronic materials (*e.g*. CD and DVD). Finally, Internet service providers and heavily frequented websites, such as search engines or auction sites, could serve as an important vehicle for pointing consumers to relevant information developed by governments and other interested parties.

Co-ordination of education and awareness initiatives

Co-ordination of education and awareness initiatives provides opportunities for enhancing their effectiveness, especially to the extent that it increases coherence and simplifies efforts. Such co-ordination can take place within and between the private and government sectors, on local, national and international platforms. Such co-ordination would help identify and expand the use of particularly effective practices. Internet service providers, for example, are in an excellent position to highlight the importance of online ID theft, and point subscribers to educational resources.

It should be noted that education and awareness initiatives are multifaceted; within government, for example, the training of persons responsible for enforcement of laws covering ID theft is an important aspect of enhancing awareness and limiting the magnitude and scope of ID theft. A number of countries are already active on this front.

International law enforcement networks such as the International Consumer Protection Enforcement Network ("ICPEN") and the London Action Plan ("LAP") could be used as platforms to help co-ordinate and disseminate educational information across OECD member countries (OECD, 2003, Section III. D).

III. Data security

Data security is also a key component of any strategy to combat ID theft. Data compromises have many harmful consequences, including exposing consumers to the threat of ID theft, exposing the entity whose system was breached to legal liability for failure to secure the data, and imposing the risk of substantial costs for all parties involved. Accordingly, member countries should develop and ensure compliance with data security safeguards, such as laws and regulations, industry standards and guidelines, and private contractual arrangements that impose data security requirements, including, if appropriate, initiating investigations and enforcement actions against entities that violate the laws governing data security.

- Member countries should better educate the private sector on safeguarding data and encourage organisations that collect and maintain sensitive consumer information to implement practical security measures to protect consumer data.

IV. Electronic authentication

Electronic authentication has been recognised as a useful process permitting the verification and management of identities on line. Under the 2006 OECD *Guidance on Electronic Authentication,* which sets out a number of operational principles aimed at helping member countries establish or modernise their approaches to authentication, the concept is understood as a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communication system. As such, it can be an effective deterrent to the theft or misuse of personal information.

Education on the benefits and proper uses of authentication are critical for user confidence on line.

As set forth in the 2007 *OECD Recommendation on Electronic Authentication* encouraging member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities, OECD countries should take steps to raise the awareness of all participants of the benefits of the use of electronic authentication at both domestic and international levels.

Electronic authentication is today considered as an element of the emerging concept of identity management. Such a broader system, which would seek to allow users to interact on line while minimising the amount of personal information they reveal on line, will be the subject of strong consideration by OECD countries in the years to come.

V. Further work

As indicated at the outset, there are three key aspects of combating online ID theft: *i*) prevention, *ii*) deterrence and *iii*) recovery and redress. This paper focused on prevention, looking specifically at ways that consumers and other stakeholders could be educated to prevent online ID theft. There is, however, a pressing need to address other aspects of the issue. Outside the OECD, the United Nations Office on Drugs and Crimes ("UNODC") is co-operating with the United Nations Commission for International Trade Law ("UNCITRAL"), developing recommendations for best practices in the prevention, deterrence, and recovery from ID theft. The European Commission is working on a harmonised definition of the concept and is considering whether online ID theft should be criminalised throughout the EU. As indicated in the *Scoping Paper on Online Identity Theft* (OECD, 2008), work is also being carried out within many OECD governments by different agencies, and by the private sector.

Some of the issues that need to be addressed at the domestic and international levels (by the OECD and other international bodies) include:

- Legal:
  - Should ID theft be defined legally as a specific offence?
  - What sorts of dissuasive sanctions might be appropriate (such as fines, confiscations, black lists, *etc.*)?
  - What legal remedies should be available for victims?
  - Should legislation require companies to take more steps to prevent identity theft, such as disclosing data security breaches affecting their customers when those breaches could result in identity theft, or improving authentication of consumers and customers when providing services or transactions?

- Cross-border enforcement co-operation between and among consumer protection enforcement authorities and the private sector.
  - How could cross-border co-operation among enforcement authorities be strengthened in the following areas?
    - Investigative and information sharing powers with foreign authorities, business and industry, consumer representatives.
    - Assistance, training, and support of other countries' law enforcement efforts.
    - Implementation and exchange of "best practices" in the area of consumer education.
- Identity recovery and redress
  - What assistance should government, industry, and/or civil society develop to help consumers restore their identity and recover from their monetary and non-monetary losses resulting from ID theft?
  - Should redress mechanisms be made available for consumers, and if so, what entities should be responsible for such redress?
  - What additional tools are needed by victims to ensure that they can restore their identity and otherwise recover fully from the identity theft?

Appendix H.1:
MULTILATERAL INSTRUMENTS ADDRESSING ONLINE ID THEFT

I. OECD instruments on E-commerce

OECD (Organisation for Economic Co-operation and Development) (1999), *Guidelines for Consumer Protection in the context of Electronic Commerce*, OECD, Paris, www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

OECD (2003), *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/consumer-policy.

II. OECD instruments in the field of security, privacy, and spam

Security:

OECD (2002), *Guidelines for the Security of Information Systems and Networks*, OECD, Paris, http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD (2007), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

Privacy:

OECD (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD, Paris, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, www.oecd.org/dataoecd/43/28/38770483.pdf.

Spam:

OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, OECD, Paris, www.oecd-antispam.org/.

III. Other international instruments

Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23 November 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

United Nation (2001), *Convention against Transnational Organised Crime*, 8 January 2001, www.unodc.org/pdf/crime/a_res_55/res5525e.pdf.

Appendix H.2:
ID THEFT EDUCATION INITIATIVES IN OECD COUNTRIES

Governmental initiatives

United States

In May 2006, the US Federal Trade Commission launched "Deter, Detect, Defend," a nationwide education campaign aimed at helping consumers take steps to reduce risks of ID theft; monitor their personal information; and quickly react when ID theft is suspected. As part of the campaign, the *ID Theft Consumer Education Kit*, helps organisations and communities inform consumers about how to reduce risks of ID theft and respond if it strikes. The kit includes:

- A booklet which provides step-by-step instruction and tools to aid in consumer education.
- A brochure.
- A 10-minute video DVD – featuring stories of how real ID theft victims responded.
- A CD-ROM containing all educational materials for easy reproduction; and
- An in-depth guidebook for ID theft victims.

In April 2007, the US President's Task Force on Identity Theft issued a report setting forth a strategic plan for addressing the challenges presented by ID theft (US FTC, US DOJ, 2007a). One focus of the strategic plan is to educate stakeholders about keeping sensitive consumer data out of the hands of ID thieves. The strategic plan recommends a multi-year public education campaign by federal, state, and local authorities. The US also established a website for information about the task force, the report, and victim's rights – http://www.idtheft.gov.

Australia

The Australian Government distributes an information kit, *How to prevent and respond to identity theft* (www.crimeprevention.gov.au), to provide the community with practical strategies on how to avoid becoming a victim of ID theft. In 2007, it released a brochure, *ID Theft: Dealing with identity theft*, as part of the Australasian Consumer Taskforce's Identity Theft Week, which operated as part of the Taskforce's annual fraud awareness campaign. The government also distributes a booklet, *E-Crime - A Crime Prevention Kit for Small Business*, which is aimed at helping small business owners identify what to do to avoid becoming a victim of

e-crime. In July 2007 the government introduced a range of e-security initiatives under the E-Security National Agenda. These include initiatives to raise awareness of e-security among home users and small business and the expansion of the national and international e-security exercise program. The government's e-security website, *Stay Smart Online* (www.staysmartonline.gov.au), provides online users with practical tips on how to secure a personal computer, smart transacting online, and information on keeping children and young people safe on line. The Australasian (Australia and New Zealand) Consumer Fraud Taskforce maintains *ScamWatch* (www.scamwatch.gov.au), a consumer scam information website providing information on several types of scams, schemes and fraud. It also provides the facility for reporting scams.

Canada

The Consumer Measures Committee ("CMC"), an organization representing federal, provincial and territorial Ministries responsible for Consumer Affairs, has developed an information kit to help consumers avoid becoming victims of identity theft, and to provide guidance on procedures to take if they do. In addition, CMC has developed a guidance document for businesses, providing them with tips on how to protect their customers' personal information (see: www.cmcweb.ca/idtheft). A number of other initiatives are carried out to inform consumers about ID theft. These include the Fraud Prevention Forum, a group of government, law enforcement and private sector organisations, which leads the annual Fraud Prevention Month campaign every March under the theme *Fraud: Recognize it. Report it. Stop it*. Identity theft, as a type of fraud, makes up a significant portion of the information that is presented to the public during Fraud Prevention Month.

United Kingdom

In the United Kingdom, the Home Office Identity Fraud Steering Committee launched the www.identity-theft.org.uk website which also contains tips about how to avoid ID theft. In addition, the Information Commissioner's Office has produced educational materials on ID theft through an information toolkit; television advertisements; and a training DVD.

Mexico

In Mexico, the public University of Mexico ("UNAM") has put in place various websites to alert consumers and users about all sorts of security risks on line. Advice on the identification of scams (www.seguridad.unam.mx/doc?ap=articulo&id=121), pharming (www.seguridad.unam.mx/usuario-casero/pharming.dsc), phishing (www.seguridad.unam.mx/usuario-casero/phishing.dsc.) and tips to prevent privacy and security breaches (www.seguridad.unam.mx/doc?ap=articulo&id=118) are provided to users.

Belgium

In Belgium, various education campaigns against Internet threats, including ID theft, are run on all kind of supports such as guides ("Guide for the Internet user"), websites (www.saferinternet.be, which targets children, http://economie.fgov.be – of the Federal Public Service Economy and which contains information on consumers' rights under Belgian laws), press releases on Internet fraud to draw consumers' attention to Internet fraud practices, such as phishing.

Japan

In Japan, the Ministry of Internal Affairs and Communications (MIC) launched an *Information Security Site for General Users* (www.soumu.go.jp/joho_tsusin/security/index.htm), a website that provides basic information on information security including countermeasures to combat online threats such as ID theft.

Industry initiatives

The private sector has also supported education initiatives in some member countries.

United Kingdom

In the United Kingdom, various banking and payment associations, such as the British Banker Association (BBA) and the UK payments Association (APACS), have pro-actively developed initiatives to educate both their own members (*i.e.* banks, and companies) and their customers; further information is available on the Internet at *www.banksafeonline.org.uk* (OFCOM, 2006, p. 37).

Netherlands

In the Netherlands, *Nederlands Vereniging van Banken*, the Dutch Banking Association, began an awareness campaign in 2006 informing consumers about ID theft risks and how to protect their personal information (INTERVICT, 2006, p. 24).

United States

In the United States, several different industries are active in educational initiatives to help fight ID theft. For example, financial institutions, which can be primary victims in a phishing attack, increasingly alert their customers about new phishing messages and security risks. Since 2004, financial institutions have undertaken joint educational efforts through the Identity Theft Assistance Center, a domestic organisation representing some of the largest US banks, brokerages, and finance companies. In addition, the National Association of Securities Dealers has published a guide entitled "Phishing and Other Online Identity Theft Scams: Don't Take the Bait." More recently, the Identity Theft Prevention and Identity Management Standards Panel ("IDSP") sponsored by the US Better Business Bureau ("BBB") and the American National Standards Institute ("ANSI") created a new

market-wide initiative that would help arm businesses and other organisations with the tools they need to combat ID theft and fraud, and protect consumers – and themselves – from the risks associated with these crimes (www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3). The report contains a catalogue of existing standards, best practices and related compliance systems germane to this issue across all market sectors and industries as well as recommendations for areas where the government and private sector should develop additional standards and guidelines. The report contains specific recommendations for consumer education initiatives in areas such as security freezes.

Australia

In Australia, the Australian Bankers' Association (ABA), the Australian High Tech Crime Centre and the Australian Securities and Investments Commission (ASIC), jointly support a website, *Protect Your Financial Identity* (www.protectfinancialid.org.au), which assists people in protecting their financial identity and minimising the damage if a problem occurs. The website contains practical prevention tips, fact sheets, and an interactive quiz allowing people to test how secure their personal details are.

Mexico

In Mexico, some members of the Internet Mexican Association ("AMIPCI") have created a website www.navegaprotegido.com.mx, which contains information aimed at educating consumers on the risks of ID theft.

Co-ordination of education initiatives

United States

In the United States for example, United States Attorney's Offices participate in ongoing training seminars, and several law enforcement agencies – including the US Department of Justice, the US Secret Service, the US FTC, and the Federal Bureau of Investigation – along with the American Association of Motor Vehicle Administrators have jointly sponsored over 20 regional, one-day training seminars on ID theft for state and local law enforcement agencies across the country (US FTC, 2007a, Vol. II, p. 71-73).

Australia

In Australia and New Zealand, the Australasian Consumer Fraud Taskforce supports a co-ordinated approach to awareness raising and education initiatives. The Taskforce was formed in March 2005 and is a group of 18 government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams. The Taskforce also has a range of community, non-government and private sector organisations as partners in the effort to increase the level of scam awareness in the community.

The purpose of the Taskforce is for the government members to work together to:

- Enhance the Australian and New Zealand governments' enforcement activity against frauds and scams.
- Run an annual coordinated information campaign for consumers: the 'Scams Awareness Month' in February or March (timed to coincide with Global Consumer Fraud Prevention Month).
- Involve the private sector in the information campaign and encourage them to share information they may have on scams and fraud.
- Generate greater interest in research on consumer frauds and scams.

Mexico

In Mexico, the eCrime working group formed by public and private entities including the Mexican Banks Association ("ABM"), the Industry Transformation National Chamber ("Canacintra"), the National Bank of Mexico ("Banamex"), the Bancomer Bank, the Mexican Internet Association ("AMIPCI"), the Preventive Federal Police, Federal Communications Commission ("COFETEL"), the National Bank and Values Commission ("CNBV"), Nic Mexico and the public University of Mexico ("UNAM"), was created to gather data on phishing trends and to cancel domain names associated with identity fraud.

Belgium

In Belgium, the Federal Public Service Economy, Small and Medium Size Enterprises, Self-employed and Energy, the Federal Computer Crime Unit of the Federal Police, and the Centre for Investigation and Information of Consumer Associations (CRIOC) organise several information campaigns targeting, among others, ID theft. For example, the *Fraud Prevention Campaign 2006* "*Arnaqué, moi? Jamais!,*" is a campaign organised within the framework of ICPEN, with a specific focus on ID theft, consumer fraud in telephone services, consumer fraud on the Internet. Information is distributed through: leaflets sent by mail or available in social services of major cities and the information shop of the Federal Public Service Economy. It is also available on the website of the Federal Public Service Economy (http://mineco.fgov.be/protection_consumer/fraud_prevention/home_fr_001.htm); the radio; press conference and publication in newsletters of external partners and newspapers; headers of credit card and telephone bills. The campaign is funded by the Federal Public Service Economy and is carried out with the help of external partners (Belgacom, National Lottery, Proximus, Mobistar, Base, Diners Club, Citibank, American Express, Europabank, Les Maisons de Justice, etc.).

Appendix H.3:
TERMINOLOGY

- *Keystroke loggers*: A keystroke logger is a program that records and "logs" how a keyboard is used. There are two types of keystroke loggers. The first type of keystroke logger requires the attacker to retrieve the logged data from the compromised system. The second type of keystroke logger actively transmits the logged data.
- *Rootkit*: A rootkit is a set of programs designed to conceal the compromise of a computer at the most privileged base or 'root' level. As with most malware, rootkits require administrative access to run effectively, and once achieved can be virtually impossible to detect.
- *Spam*: There appears to be a growing correlation between malware, phishing, and spam. Spam is commonly understood to mean unsolicited, unwanted and harmful electronic messages.
- *Trojan horses*: A Trojan horse is a computer program that appears legitimate but which actually has hidden functionality used to circumvent security measures and carry out attacks. Typically a Trojan enters a user's computer by exploiting a browser vulnerability or feature.
- *Virus*: A virus is a hidden software program that spreads by infecting another program and inserting a copy of itself into that program. A virus requires a host program to run before the virus can become active. The term "virus" is increasingly used more generically to refer to both viruses and worms.

BIBLIOGRAPHY

ANSI (American National Standards Institute) and BBB (Better Business Bureau) (2008) ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel Final Report, 31 January 2008, www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3.

BWGCBMMF (2004), *Report on Identity Theft*, report to the Ministry of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2004, www.ps-sp.gc.ca/prg/le/bs/report-en.asp.

EC (European Commission) (2006), DG SANCO, *Special Eurobarometer*, *Consumer Protection in the Internal Market*, September 2006, Brussels, http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf.

FTC (Federal Trade Commission) and DOJ (Department of Justice) (US) (2007a), *Combating Identity Theft: A Strategic Plan*, US President's Task Force on Identity Theft, 23 April 2007, www.idtheft.gov.

FTC (2007b), Report on *Consumer Fraud and Identity Theft Complaint Data*, www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

INTERVICT (International Victimology Institute Tilburg) (2006), *The Challenge of Countering Identity Theft*, Report Commissioned by the National Infrastructure Cyber Crime program ("NICC"), 6 September 2006, www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf.

ITU (International Telecommunication Union) (2006), *Cybersecurity Awareness Survey*, results as of 17 May 2006, www.itu.int/newsroom/wtd/2006/survey/charts/q_8.asp.

McAfee (2006), *Virtual Criminality Report*, December 2006, www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

OECD (Organisation for Economic Co-operation and Development) (1999), *Guidelines for Consumer Protection in the context of Electronic Commerce*, OECD, Paris, www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

OECD (2003), *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/crossborderfraud.

OECD (2006a), *Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/dataoecd/45/53/37125909.pdf.

OECD (2006b), *Mobile Commerce*, DSTI/CP(2006)7/FINAL, Directorate for Science, Technology and Industry, www.oecd.org/sti/consumer-policy.

OECD (2006c), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, OECD, Paris, www.oecd-antispam.org/.

OECD (2007), *Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, www.oecd.org/dataoecd/43/50/38960101.pdf.

OECD (2008), *Scoping Paper on Online Identity Theft*, DSTI/CP(2007)3/FINAL, Directorate for Science, Technology and Industry.

OFCOM (Office of Communications) (UK) (2006), *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, 21 June 2006, www.ofcom.org.uk/research/technology/onlineprotection/report.pdf.

Annex I.
OECD POLICY GUIDANCE FOR ADDRESSING EMERGING CONSUMER PROTECTION AND EMPOWERMENT ISSUES IN MOBILE COMMERCE

I. Introduction

Mobile commerce developments

For the purposes of this document, mobile commerce, also known as "mobile e-commerce" or "m-commerce," means commercial transactions and communication activities conducted through wireless communication services and networks by means of short message services ("SMS"), multimedia messaging service ("MMS"), or the Internet, using small, handheld mobile devices that typically have been used for telephonic communications. "Mobile operator" refers to a company that provides services to mobile subscribers; "mobile vendor" refers to a company that sells goods and services through mobile platforms, either directly, or through intermediaries including website operators (such as Yahoo! and eBay) and mobile aggregators (*i.e.* entities that assist mobile vendors by, for example, processing and forwarding multiple third-party vendor charges to mobile operators for billing to mobile subscribers); "mobile subscriber" refers to the individual who pays for a mobile phone subscription.

With the convergence of operating platforms, mobile commerce is now expanding into Internet-based e-commerce. This is making it increasingly difficult to distinguish mobile commerce from other forms of e-commerce. While mobile commerce does not as such require Internet access, ever more m-commerce transactions occur by means of communications system protocols (such as Web (HTML, TCP/IP), Wireless Application Protocol ("WAP") and i-mode) and phones connected to wireless communications networks (*e.g.* "3G"). In addition, an increasing number of personal data devices or smart phones are now able to support wireless telephonic communications.

Mobile commerce is currently growing at a rapid pace in many OECD countries. In these countries, more and more individuals have advanced mobile phones and other such devices that allow them to benefit from a broad range of mobile services that are different from what is currently possible from fixed computers. Between 1997 and 2005, the number of mobile subscribers in the OECD grew at an average compound growth rate of 24% per year (OECD, 2007b, p. 98).

Currently, mobile phone subscribers can use their devices:

- To purchase and download content, such as movies, music, ring-tones, or games.
- To play online games and gamble online.
- To access information available on a mobile screen, such as weather forecasts or the news, mobile TV and program-related information broadcast alongside TV channels.

- To obtain information tailored to data about their location through location technology.
- To access online banking and financial services, and make transactions.
- To make payments for mobile activities, either charged on credit cards or on mobile phone bills.
- As payment devices ("e-wallet") to purchase goods or services; and
- To vote in interactive TV programmes.

The development of the third generation of mobile services ("3G"), which provides high-speed Internet access on mobile phones, complete with audio and higher quality graphics, has expanded consumers' interest in the devices and opened up the potential of new commercial applications.

Another development concerns the increasing access and use of mobile phones by children. Ensuring that children benefit from mobile devices' opportunities while receiving effective protection against aggressive, inappropriate and abusive mobile marketing practices and offers represents a key challenge for all stakeholders.

Emerging mobile commerce challenges for consumers

The Committee on Consumer Policy (CCP) has been following developments in mobile commerce for a number of years. In 2007, the Committee issued a report (OECD, 2007a) providing an overview of m-commerce and identifying some of the key challenges it would pose to consumers. The report notes that mobile devices have unique characteristics that attract consumers' interest (they are easy to use and offer consumers access to service whenever they want from areas where mobile service is available), but that they also present inherent technical constraints such as small screen size, limited storage and memory capacity, battery life, and low processing power.

This document aims at providing practical measures that stakeholders could take to address a number of key issues that have emerged in countries where the market is well advanced. Other issues may well emerge over time. This document is therefore not designed to provide a comprehensive set of policy principles and actions, but rather offers some principles to guide an evolving exploration and analysis of current and future challenges posed by m-commerce. These challenges are presented below in the form of hypothetical examples.

The Committee decided to focus on three issues:

- The problems that could occur as a result of limited information disclosure possibilities on mobile devices (due to the small screens and other technical limitations).
- The increased risks of commercial exploitation of minors; and
- The heightened vulnerability of mobile devices to unauthorised use, data security breaches and privacy risks.

The Committee decided to examine these issues in light of the 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("the *E-commerce Guidelines*") (OECD, 1999). While most delegations considered that the

principles contained in the *E-commerce Guidelines* apply to m-commerce, they recognised that it would be beneficial to elaborate on how these principles could be effectively applied by mobile operators, website operators, mobile aggregators and mobile vendors of financial and other commercial services, as well as mobile subscribers, to address the issues mentioned above. In doing so, the Committee would also incorporate best practices from other relevant OECD instruments pertaining to consumer protection, security, privacy and spam (as listed in Appendix I.2).

II. Limited information disclosure

The *E-commerce Guidelines* indicate that consumers should be provided with information, prior to contracting, to enable them to make informed decisions in their electronic transactions. Such information, which should be accurate and easily accessible at all times, is as follows (see box below):

- Information on the business and on available dispute resolution mechanisms.
- Characteristics of the goods or services on offer; and
- Details about the transaction itself, including the terms, conditions and methods of payment, and costs.

Key disclosure provisions in the E-commerce Guidelines

Part II of the E-commerce Guidelines set forth the following general principles:

- Section II ("Fair Business, Advertising and Marketing Practices") sets forth several general principles stating that businesses should not engage in practices that are likely to be deceptive, misleading, fraudulent or unfair; that businesses marketing to consumers should not engage in practices that are likely to cause unreasonable risk of harm to consumers; and that businesses should present information about themselves and the goods or services they provide in a clear, conspicuous, accurate, and easily accessible manner.
- Section III, C ("Online Disclosures - information about the transaction") states that the business should provide sufficient information about the terms, conditions, and costs associated with a transaction to enable the consumer to make an informed decision about whether to enter into the transaction. The information must be clear, accurate, and easily accessible and include "an itemisation of total costs collected and/or imposed by the business."
- Section IV ("Confirmation process") indicates that there should be a way for consumers to review the purchase details and make an express, informed and deliberate consent to complete the transaction. It also states that consumers should be able to retain a complete and accurate record of the transaction. They should finally be able to cancel the transaction process before concluding it.
- Section VI ("Dispute Resolution and Redress") encourages businesses to provide consumers with fair, effective, transparent and internal mechanisms to address complaints. In this regard, the *2007 OECD Recommendation on Consumer Dispute Resolution and Redress* calls on the private sector to establish "[e]ffective processes for internal complaints handling, which provide consumers with the opportunity to resolve their complaints directly with the business concerned in a fair, effective, and timely manner without imposing a fee or charge for accessing or using these processes."

Providing such comprehensive information to consumers is complicated in the case of m-commerce due to mobile devices' inherent technical constraints such as small screen size and, in many devices, limited memory or storage capacity. Mobile phone offers for services or goods have typically been made in the form of SMS or mobile e-mail. In addition, they may also appear through Internet websites accessed on mobile devices. With the increased linkage of mobile devices to the Internet, even if information requirements can be technically met, they may not be sufficiently accessible to mobile phone subscribers for technical reasons.

Access to information about businesses, goods and services, and the transaction process

Offer for TV

An e-commerce retailer sent an offer for a TV to one of its customers on his mobile phone. The offer indicated that full information about the company, the TV and the terms and conditions of the sale were available on the company's website, and provided the URL. The customer ordered the item without consulting the webpage. When he received the bill, he was surprised at the high shipping and handling charges. He complained to the company, but was informed that the full details on costs were provided on the website.

In the above case, the mobile vendor seems to comply with the information requirements contained in Section III, Part II of the *E-commerce Guidelines*. However, there may be questions as to whether the information, which is only available on the Internet, would be sufficiently accessible by mobile phone subscribers. Some consumers may not have Internet access on either their mobile phones or computers. In response, governments could, acting under other provisions of the *E-commerce Guidelines*, such as Part III ("Implementation"), encourage mobile vendors to:

- Provide basic pre-contractual information by SMS, recognising that this is only a partial solution due to current limitations communications providers have made on the length of such messages and the inability to print out such information.
- Mail complete information in written form to the mobile phone subscriber expressing interest in the commercial offer.
- Provide a phone number that consumers could call to get more detailed information about their purchases.

In addition, governments could seek to address these issues by:

- Promoting self-regulatory schemes and best practices, and encouraging private sector leadership in the development of technology to ensure that consumers can easily access the full information they need to determine whether to make a transaction.

In the future, technology aimed at providing wireless data over long distances may be helpful to the extent it facilitates transfer of data between mobile devices and computers.

Confirmation process

Unwanted subscription

A consumer using a mobile phone reached a website offering a one month free online access to a business magazine. He provided his details through SMS to accept the offer. He did not however notice the contract terms that were at the bottom of the page. They stated that after one month he would have to pay for the service; viewing the terms would have required extensive scrolling. The consumer was puzzled two months later when he received his mobile phone bill by SMS, which included a charge for the above service; he did not recall indicating that he wanted to subscribe to it at the end of the trial period.

In the above example, the consumer accessed a site, but did not confirm his intent to subscribe to that service at the end of the trial period. The service provider nonetheless claimed that the consumer had ordered the service.

The above scenario suggests that mobile phone subscribers should be given the opportunity to receive clear and full information about the proposed transaction prior to the conclusion of the contract so that they can confirm the goods or services ordered, correct any errors and to retain or print out adequate records of the proposed transaction made over mobile devices, including contract terms (*E-commerce Guidelines*, Part II, Section II and IV). If a mobile subscriber does not receive such prior information, it might be beneficial to:

- Provide mobile subscribers with an opportunity, in mobile transactions, to withdraw from the transaction process until such time as they have been provided with the possibility to review the full contract and express an informed and deliberate consent to the purchase.

In addition, mobile phone subscribers should be protected against unfair or unscrupulous mobile vendors who may, through information they obtain about the identities of persons visiting their site, exploit or harass them. To protect mobile phone subscribers from such risks, rules restricting the information (other than directory information such as name and phone number) that mobile operators can disclose without the customer's permission, to outside parties including to joint venture partners or independent contractors for marketing purposes, could be put in place in jurisdictions where existing protection is not adequate. Other mechanisms, such as rules mandating conspicuous disclosure of a mobile operator's data collection practices, could also be considered.

Stock purchase

A consumer signed on to his bank to place an order to sell stock over a mobile phone. He validated the details of the order, thinking he had confirmed the transaction. He did not realise that he had to scroll to the bottom of the validation page for confirmation information. The process for confirming the order was not clearly indicated; as a result, the transaction was not executed.

In the above example, the financial service provider had informed the consumer about the need to carry out the transaction, but in doing so, had failed to give the opportunity to confirm it. Care needs to be taken to ensure that the procedures for carrying out transactions on mobile handsets take the limitations of screen size and

storage capacity into account. Once basic information on an order has been supplied, it would be beneficial for consumers to:

- Receive confirmation of a transaction via an SMS message or e-mail.
- Provide a way for consumers to easily check on the status of their order, on their mobile handset as well as on the Internet.

Dispute resolution and redress

Section VI, Part II of the *E-commerce Guidelines* ("Dispute Resolution and Redress") encourages businesses to have fair, effective, transparent and internal mechanisms to address complaints. This principle is developed further in the 2007 *OECD Recommendation on Consumer Dispute Resolution and Redress*, which calls upon private sector participants to establish "[e]ffective processes for internal complaints handling, which provide consumers with the opportunity to resolve their complaints directly with the business concerned in a fair, effective, and timely manner without imposing a fee or charge for accessing or using these processes."

Complex chains of contracts

Interactive TV

A television talent show invited viewers to vote for their favourite contestants by sending short codes through their mobile handsets. The price of the call was disclosed only at the bottom of the screen in fine print that appeared for 10 seconds. Moreover, the print was impossible to read from the distance that viewers would normally sit from their television screens. There was no confirmation process sent on their mobile phones – after voting, viewers simply saw a message thanking them for their votes. Mobile subscribers did not realize that they had been billed for premium rate (above the cost of standard transmission) messaging services until the charges appeared on their mobile service bills. When they disputed the charges with their mobile service operators, they were informed that they had to pay the bill and take the problem up themselves with the television programme.

Mobile handset transport ticket

A consumer ordered a transport ticket from the national railway company via his mobile handset, allowing him to use his Near Field Communication enabled handset as his ticket on local buses, trains, and trams. While he was on a tram, he was stopped by a controller, who tried unsuccessfully to validate the m-ticket. As a result, the controller required him to pay for the ticket immediately and levied an additional fine because the consumer was unable to prove that he had purchased the ticket. Back home, the consumer asked his mobile operator for assistance with reimbursement for the second ticket and the fine.

The mobile operator informed him that it was not responsible in this matter and that the consumer should send his request to the railway company.

The first hypothetical case shows the interaction between two media – traditional television and commerce carried out through mobile devices. It highlights the trend towards using premium text messaging as a business model in m-commerce. The hypothetical case also raises a number of issues for mobile subscribers including: *i*) the inability of consumers to know when they are accessing premium messaging services on the mobile handsets, *ii*) the lack of a confirmation

process, and *iii*) the mobile operator's lack of an effective dispute resolution and redress system for the billing dispute.

With respect to dispute resolution, both examples illustrate a case where there is a lack of clarity as to which entity is directly responsible for handling consumers' claims. Typically, charges for mobile commerce transactions are billed to mobile subscribers by the consumer's mobile operator on behalf of the vendor of the goods or services through mobile platforms. In some cases, relationships in the delivery of m-commerce services are even more complex, notably when payment for the service at offer is debited from the consumer's bank account or credit card, as shown in the second example above.

In a few OECD countries, partnerships have been established or are being established between transport companies and mobile operators to provide consumers with the ability to use their mobile handset as a transport ticket. In these countries, consumers are charged by several methods: on their mobile phone bills, their credit cards or via cash transactions. In these multi-dimensional transactions, it should be clear to the consumer which entity has responsibility for handling consumer disputes and providing redress.

The two examples above suggest that it might be beneficial to encourage mobile operators and vendors to:

- Establish fair, effective and transparent internal mechanisms to address and respond to consumer complaints.
- Clearly indicate to consumers rules on responsibility for handling claims in complex contracts. Best practices could, in this regard, provide guidance on who, between the mobile operator, transport company or both, is accountable to consumers in light of the specific circumstances and characteristics of a case.

Moreover, m-commerce participants should consider implementing dispute resolution and redress mechanisms such as customer satisfaction codes, chargeback mechanisms, and alternative dispute resolution services, as recommended in the *2007 OECD Consumer Dispute Resolution and Redress Recommendation* ("the *Consumer Dispute Resolution and Redress Recommendation,"* Annex, Section II, A.7).

It would be beneficial for mobile operators, mobile vendors, website operators, mobile aggregators and governments to work together to establish fair, effective and transparent self-regulatory mechanisms, policies, and procedures to address consumer complaints and resolve consumer disputes arising from complex m-commerce transactions.

Cross-border disputes

Luxurious watch

A consumer received an SMS containing a link to a website, which advertised a luxurious watch at a low price. The consumer felt confident that the offer was genuine because it came from a mobile site from which he had already bought similar products and which contained information in his native language. He therefore placed an order to buy the watch. When the watch was not delivered, the consumer complained to the customer service department of the company, and found out that the business that he purchased the item from was in fact operated by another company which was not based in his country. When he complained to government authorities, he was told that they could do nothing since the business was located outside the country.

Part II, Section III, A *i*) and *iii*) of the *E-Commerce Guidelines* requires businesses to provide consumers with accurate, clear and easily accessible information about themselves (including their geographic locations) and ways to resolve disputes. Such information and redress mechanisms are necessary to help strengthen consumer confidence in cross-border transactions, as also provided for in the *Consumer Dispute Resolution and Redress Recommendation* which calls on member countries to enhance the effectiveness of consumer remedies in cross-border disputes (Annex, Section III).

Stakeholders are encouraged to establish effective dispute resolution mechanisms to address consumer complaints in cross-border m-commerce transactions.

Access to m-commerce for disadvantaged consumers

As recommended in the *Consumer Dispute Resolution and Redress Recommendation* (Annex, Section II, A. 6), the special needs of disadvantaged consumers should be addressed as m-commerce develops. For example, it may be particularly problematic for people with low vision to review disclosure/disclaimer statements on small mobile screens.

III. Protection of minors

In most OECD member countries, minors (*i.e.* generally persons under the age of 18) do not have the legal capacity to enter into commercial contracts – including, for example, contracts for voice calls or commercial transactions over their mobile devices. This does not, however, necessarily prevent them from engaging in commercial transactions using a device that is part of a contract entered into by their parents or another adult. In some countries, older minors may, however, be allowed to conclude such contracts, provided that they obtain prior parental consent. This parental control over minors' commercial activities is currently being challenged in the mobile commerce marketplace due to the sharp increase in the number of minors who possess their own devices (OECD 2006, p. 5-6). One way of discouraging minors from falsely entering into contracts would be to:

- Encourage mobile operators to put age verification systems in place.

To date, however, age verification technologies have failed to develop on a widespread basis. This is a challenging problem. Mobile operators can seek age information in a manner that discourages age falsification, *e.g*. by requiring children to enter their birthdates, rather than their actual ages. However, in the absence of age verification technologies, it is not difficult for children to evade a site's age screening mechanisms by submitting false age information, thereby gaining entrance to inappropriate sites and/or engaging in transactions without parental authorisation. This highlights the need for supplementary technology that can provide additional measures of security for children as, more and more, they engage in online activities from wireless handsets.

While parents usually aim to provide their children with mobile phones to improve communication and enhance safety, children's use of mobile phones goes much further (OECD, 2006, p. 8). They are increasingly attracted by services to which fees may be attached (such as ringtone downloads, videos, chatting, and games). As a result, they are engaging in commercial transactions, and may be exposed to risks such as *i*) access to harmful or adult content and *ii*) unexpectedly costly transactions which could result from aggressive marketing.

Part II, Section II of the *E-commerce Guidelines* provides that "Businesses should take special care in advertising or marketing that is targeted to children, …, who may not have the capacity to fully understand the information with which they are presented." This principle should guide mobile service providers, mobile operators, and others offering m-commerce services in communications and transactions with children.

Access to harmful or adult content

For adults only

A 15-year old received a text message inviting him to preview a new Internet site for free. He responded to the message and acquired the site address in return. He accessed the site, discovering that it contained sexually explicit material. He reported the offer to his mother, who contacted the mobile operator immediately, to express her outrage that her child had received the solicitation. The mobile operator explained that it did its best to filter such traffic, but some inappropriate content slipped through. When the child responded to the SMS, his contact information (i.e. phone number) was put on a list of potential customers. He subsequently received a stream of provocative messages, forcing the distraught mother to demand a new mobile phone account for her son.

Free photo site

A 15-year-old found out about a website offering adult-oriented photos for free from his friends. He went to the site using his mobile phone, knowing his parents would not be able to monitor his web activity closely. The website contained a warning that users should be over the age of 18. He responded that he was, and was granted instant access.

Businesses should consider developing more effective tools to prevent minors from accessing adult content sites from their mobile platforms. As stated in the *E-commerce Guidelines*, member countries "should… encourage continued private sector leadership in the development of technology as a tool to protect… consumers" (Part III, *iii*), "Implementation").

Much has been done to develop software that does just that with respect to screening certain content from consumers who use their computers to access the Internet. To address this issue in the m-commerce environment, voluntary codes of conduct or guidelines have been developed by mobile operators in some countries to put in place options for restricting children's access to adult content (Appendix I.1). Under these frameworks, mobile operators have supported a number of ways to respond to issues involving minors, including:

- The development of awareness-raising campaigns for parents and children.
- Warning in all audio and visual advertising that interested parties must be 18 or older or have a parent's permission to participate.
- The classification of commercial content (restricted adult content versus generally accessible content); and
- The development of more effective age verification procedures.

Additional measures that could be explored to protect minors include:

- Adapting existing member country laws and rules protecting children on line to the mobile environment.
- Encouraging mobile operators to inform parents of the filtering options available to them to help prevent children's access to adult content.
- Encouraging mobile vendors selling adult content services *i*) to work with the relevant authorities at domestic level to ensure effective protection of minors and *ii*) to put in place appropriate safeguards to prevent children's access to these services.
- Establishing procedures under which, for example, a notice could be sent to parents if their children access adult content sites; and
- Filtering services that could be activated by parents on the device to block Internet access to inappropriate content.

Marketing targeting children

Ring tones and related items

A 13-year-old was intrigued by various messages she received on her mobile handset from a vendor from whom she had previously bought a ringtone. The vendor encouraged her to buy all sorts of goods and services. She ended up buying a number of additional ringtones, games, and horoscopes. Her mother asked the mobile operator to intercept the ads, but it indicated that it was powerless to do so.

Unsolicited ads

A ten-year-old was shopping in the mall with his mother. As they walked past stores he was intrigued by the ads that were being beamed to him on his mobile phone by the different retailers. He showed his mother, who was impressed by this new phone feature. She was unaware of the properties of the Bluetooth technology that was installed on her son's device. When they returned home, the mother became concerned that there might be downsides to the unsolicited advertising that was now possible through the Bluetooth technology.

As set out in the *E-commerce Guidelines* (Part II, Section II), children may not have the capacity to understand fully the information that they are presented. While it may be difficult to prevent abusive m-commerce marketing that targets children, there might be possibilities for limiting it by encouraging mobile operators to put in place tools that would:

- Educate parents along with their children about aggressive marketing techniques and ways to keep spending through mobile devices in check.
- Block certain advertisers, or types of advertisers, from sending solicitations to children.
- Place restrictions on Internet content access.
- Block mobile phone purchases on devices given to children who are minors; or
- Block all mobile messages other than those from sources parents identify (known as a white list).

Mobile vendors could also be encouraged to require adult authorisation for any m-commerce purchases from parties they know to be minors.

The "Unsolicited ads" example raises a different type of challenge; in this instance, ads were beamed to the child's phone using Bluetooth technology. Such advertising was not conducted through a mobile operator and was unrecorded. The example shows that parents need to be aware of the technological capabilities and features of the mobile phone device used by their children. They need to know how these features can be modified when concerns arise.

Over-consumption of services offered by mobile operators

Soft drink vending machine

A 12-year-old girl was delighted when she was elected president of her sixth grade class. At the lunch break, she decided to express her appreciation by buying a round of soft drinks for her classmates. The word spread rapidly, and soon there were 300 young friends waiting to be treated. She used her mobile phone to pay for the drinks. The total charge appeared on her mobile screen. When the monthly statement arrived at her home, her father was stunned to see the EUR 400 charge.

Interactive games

A 16-year-old received a mobile phone for his birthday. His mother lectured him about not running up large charges. The young man agreed, and tried to stick to his word. However, as he saw that text messages and interactive games were very cheap, he used the services extensively, not realising that the many small charges were adding up to a tidy sum. The total monthly bill topped USD 200.

As seen in the examples above, parents may not be in a position to supervise their children's activities on their mobile handsets at all times. As a result, they may not be able to prevent them from running up substantial charges on their phone bills for services or products purchased. TV games and competitions are areas in which minors seem particularly vulnerable. As illustrated earlier in the *Interactive TV*

example, information on the costs of participation in such games is not always clearly available.

Vending machines in school premises or shopping centres are another example of temptations for minors. From their mobile phone, minors can sometimes call up a phone number indicated on the vending machine, and pay for their purchase, which will then appear on their next phone bill.

Premium rate services, as discussed earlier, may also represent temptations for young consumers. These services offer information and entertainment through a variety of media including fixed phone, fax, Internet, TV and mobile devices. Children can thus easily make a call from their mobile handset to access a wide range of services ranging from competitions, chat lines, *etc.* Typically, premium rate service calls are charged at a higher rate than standard calls. Industry can help by continuing to develop and refine technological tools to limit consumption of mobile services by minors. Such tools would be consistent with the *E-commerce Guidelines* (Part II, Section III, C. *v*) which call on businesses to provide consumers with information on the restrictions, limitations or conditions of purchase, such as parental/guardian approval requirements, geographic or time restrictions.

The approach used by credit card companies may be relevant in this regard. Once a card has been issued to an individual, the companies often allow, with the individual's consent, additional cards to be issued to other family members, under the credit limit of the principal subscriber. Credit lines can be limited and bills are sent to the principal for payment. Moreover, in some countries, minors cannot hold a credit card unless parents provide special agreement to the contract.

A few countries have gone much further (Appendix I.1), placing greater responsibility on mobile operators. In one country, in the case of TV games in which participation is through SMS, mobile operators must reimburse parents for bills incurred by their children. In another country, content providers who do not set a monthly limit for the purchase of services from an access number may be considered in breach of the law.

To help prevent over-consumption by minors, stakeholders could:

- Provide parents with the ability to set a ceiling that would limit the amount of charges that children could accrue using mobile phones, by, for example, setting a limit on the number of text messages, or establishing monetary limits on downloadable purchases.
- Encourage mobile devices to be designed in a way that users could limit the types of transactions.
- Encourage mobile operators to send warnings/notices to parents when expenditures exceed an established ceiling level.

Children and location-based data[1]

Keeping track

A 12-year-old mobile phone user goes on the Internet and enters her mobile phone number to sign up for a location-based service that allows her to receive information about the location of persons she has identified (social mapping). She believes this will be a fun chance to find out when her school friends are in the area so she can text message them and meet up with them. They can also receive location data and a profile about her. There is no disclosure about how such information will be safeguarded, or who can view it. There is no verification process. The location data is not blocked even when she turns off that program on the mobile device. Her parents do not know she has subscribed to such a service.

The above example illustrates challenges raised by the intersections between privacy, online activity and mobile commerce as they affect children. Other, related privacy issues, which may affect both children and adults, are discussed below in the section on "Location-based privacy and security issues". In many OECD countries, the disclosure of certain types of location-based data to third parties is illegal; however, there are still open issues regarding the extent of such protection in some countries. The lack of disclosure about tracking and the sharing of the data with third parties is magnified in many countries by the absence of a process to alert adults about these practices. Although fuller disclosure might help address the problem, it would not be sufficient.

The *E-commerce Guidelines* already set forth several general principles that might apply, including the principle that businesses marketing to consumers should not engage in practices that are likely to cause unreasonable risk of harm to consumers (Section II, Part II, 2nd paragraph); and that businesses should present information about themselves and the goods or services they provide in a clear, conspicuous, accurate, and easily accessible manner (Section II, Part II, 3rd paragraph). Here, tracking information might be considered in following the principle that the business should provide sufficient information about the terms, conditions, and costs associated with a transaction to enable the consumer to make an informed decision about whether to enter into the transaction. Such information must be clear, accurate, and easily accessible. As mentioned above, the *E-commerce Guidelines* also encourage private sector leadership in the development of technology as a tool to protect and empower consumers (Part III, *iii*)). To that end, businesses could:

- Make clear disclosures about tracking.
- Make clear disclosures about the sharing of data with third parties and how to limit it.
- Treat this as a service for which adult approval is required.
- Provide the option to turn off the specific tracking service, preferably as a default.

1. Location-based data concerns information indicating the geographical location and movement information of a mobile device.

IV. Unauthorised use of mobile handsets and security issues

The small size and functionality of mobile devices have made them attractive targets for thieves, who may be interested in *i*) re-using or re-selling the device, *ii*) carrying out commercial transactions in a fraudulent or illegal way in the name of the legitimate owner or *iii*) obtaining sensitive personal information. The risk of theft is in many ways far higher than for standard computers, which are stationary or bulkier portable computers, which are not carried around in public to the same degree.

Unauthorised use of mobile phones

Building awareness of the risks of unauthorised use of mobile phones should help to lower the number of incidents. As provided for in Section VIII, Part II, of the *E-commerce Guidelines,* stakeholders "…should work together to educate consumers about electronic commerce … to increase … consumer awareness of the consumer protection framework that applies to their online activities." Educating consumers as to what they should do in the event their mobile devices are stolen or compromised is another important aspect of preventing fraudulent use. Stakeholders should therefore work together:

- To provide information to consumers that *i*) promotes awareness; *ii*) outlines ways to protect mobile devices from loss and misuse; and *iii*) indicates what consumers should do if they discover their device has been lost or is being misused.

Buying spree

A consumer loses his mobile phone without however informing either his mobile operator or the police about it, hoping that he will find it quickly. Three days later, the police call the consumer to let him know that his phone was found. However, from the moment the phone was lost to the time that the police found it, someone used expensive mobile services from the phone, running up charges of around USD 2 000. The consumer is shocked to learn that he is liable for the full amount.

The above example underscores the importance of using the security offered by some form of encryption on the device itself as well as a PIN for some services. It also underscores the importance of timely notification when a mobile device is missing. Further possibilities to limit liability in the event of theft include:

- Enabling consumers to establish credit ceilings that may be lower than the limited liability ceilings set by handset operators.
- Providing on-demand remote services or other technical devices to enable consumers to freeze a device to prevent unauthorised use.
- Requiring that a PIN code be used for each commercial transaction carried out using the mobile device, or for accessing sensitive information on the handset.
- Educating consumers about the significance of using passwords and other technology for limiting access to such devices.

With respect to the PIN code of the SIM card, in general "0000" is assigned as an initial default PIN number.[2]

- To help deter unauthorised use, mobile operators and mobile device merchants could *i*) assign random numbers as initial PIN codes and/or *ii*) prompt consumers to change their default PIN code and set their own when they first use the device.

Busy signal

A young woman lost her mobile phone on the bus as she was returning home from work. When she discovered the theft, she immediately called her mobile operator. Several times, the line was busy. Other times, she gave up after waiting for 20 minutes for a customer representative. She was infuriated several days later when she learned that the phone had been used to purchase about EUR 1 000 of services during the time she had tried to contact the mobile operator.

Holding mobile subscribers liable for unauthorised charges made using stolen mobile devices, during a period when the subscribers were unable to notify their operator of the theft because of busy lines and the like raises questions of fairness. The inaccessibility could expose the subscribers to unreasonable risk of harm, which is inconsistent with the E-commerce Guidelines, and with the Consumer Dispute Resolution and Redress Recommendation (Part IV), which calls on the private sector to provide mechanisms for consumers to resolve their disputes at the earliest possible stages. To avoid such situations, mobile operators could be encouraged to:

- Provide sufficient means for subscribers to report their troubles easily, including, for example, through an e-mail or "online" facility for declaring lost or stolen devices.
- Set up special reporting lines for lost and stolen handsets where consumers could "key-in" information to disable the handsets.

Efforts to improve the reporting mechanisms for lost handsets have been made in a number of countries. In one country, mobile operators have teamed up and signed a charter to block cell phones reported stolen on all their networks within 48 hours. Since mobile handsets are equipped with a registered international mobile equipment identification ("IMEI") number,[3] each of the companies can place a bar on the SIM card and the IMEI via remote control to lock the handset and make it inoperable.

It should be noted that in instances where a mobile phone is used as a payment device, liability often differs from that related to the use of credit cards. In some OECD countries, consumers are, in many instances, not liable for amounts debited from a stolen credit card. When mobile phones are used as payments devices, mobile subscribers are not guaranteed the same level of protection. Mobile operators in most member countries do not cover any loss caused by the unauthorised use of SIM cards or IC chips. However, a few countries amended their legislation so as to limit the liability

2. This would not apply to the Code Division Multiple Access (CDMA) network technology, which is used for mobile phones in some OECD countries.

3. Mobile handsets using the CDMA network technology are equipped with an Electronic Serial Number (ESN), which, like IMEI, is used to identify a unique mobile device.

arising from all types of unauthorised use of communication services. To address the problem, governments and industry may want to:

- Explore whether there could be ways to enhance liability protection for those using mobile phones; as the *E-commerce Guidelines* and the *Consumer Dispute Resolution and Redress Recommendation* state, limitation of consumer liability and chargeback mechanisms offer powerful tools that could help protect consumers.

Foreign vacation

A woman who was spending her summer vacation in a foreign country had her mobile phone stolen from her while she was shopping in an open market. She regretted the loss but was not concerned about it being misused because the mobile operator had told her that her phone would not work in foreign countries as it was not compatible with the telecommunications network. She therefore did not report the loss, until she returned home. The mobile operator informed her of the bad news. Some USD 20 000 had been charged to her account. While it was true that her phone would not work abroad, the mobile operator had failed to tell her that the IC chip (or SIM card) could be removed from her phone and used in a different device. The company admitted that this was not clear in the information packet that they provided to her, but insisted that she pay. She took them to court where she won her case.

In the above example, the mobile operator should have provided its customer with complete information on the operation of her IC chip in foreign countries. As prescribed in Section V, Part II of the *E-commerce Guidelines*, consumers should be provided with secure payment mechanisms and information on the level of security afforded by the mechanisms. This principle is particularly important as ever more consumers use their mobile handset abroad. Efforts should therefore be made to:

- Ensure that mobile subscribers receive clear and complete information on how their mobile devices can, or cannot, be operated in foreign countries at the time they purchase their devices; and
- Warn mobile subscribers, when they purchase their mobile phone, that the IC chip of the device may be used by an unauthorised person even if the device itself may not be used abroad.

Bad loan

An office mate used his colleague's mobile device and phone number to transact a loan without authorisation. To conclude the loan, the office mate sent a message indicating the subscriber's name. The loan company did not check further the identity of the sender.

Allowing parties to use their mobile handsets to make purchases in the name of someone deviates from Section V of the *E-commerce Guidelines* on two key points: *i*) security of payments and *ii*) fair business, advertising and marketing practices (since the practice raises unreasonable risk of harm to consumers). To prevent such practice, it might be beneficial for business to put in place security procedures and tools to help identify a party in a contract concluded over a mobile device. This could be addressed, to some extent, by:

- Limiting a purchase order to the party who holds the account on the handset from which such an order is placed.
- Verifying a subscribers' identity by using information such as an SMS, a mobile e-mail address, or a PIN code.

Mobile security

Mobile banking breach

A mobile phone subscriber received an advertisement for free mobile banking services claiming that consumers could access the application anywhere and at any time with just one click. The advertisement stated that consumers could view account balances, transfer funds between accounts, and receive and pay bills, just as they do now using their home computer. It claimed that to help ensure privacy and security, all information on the mobile banking application was password-protected and encrypted and further claimed that it would protect the consumer against any unauthorised transaction. The ad contained a link to the application form, which was sent via text message. The mobile subscriber completed the application, signed up for the service, and began using it.

The next month, the mobile subscriber received a bill from her banking service provider that contained significant charges for the application and for accessing her banking data by handset. The bank's advertisements did not disclose these charges. The following month, the consumer learned that an unauthorised debit has occurred on the bank account. She attempted to have the mobile operator delete the charge but it referred her to the bank, explaining that after investigation, it appeared that the consumer's banking data had not been secured and had been compromised.

This hypothetical case raises issues for consumers including: *i*) the security of mobile handsets, particularly as payment devices; *ii*) disclosure of the costs of data access charges; and *iii*) access to appropriate dispute resolution and redress mechanisms. This section focuses on the wireless security/consumer protection issues as the other two issues are discussed above, in relation to the *Interactive TV*, *Mobile handset transport ticket* and *Luxurious watch* hypothetical examples.

Mobile devices are increasingly becoming mini-computers, which are capable of carrying out a growing range of operations, including mobile banking. The security of the wireless networks supporting the devices, both in laptops and smaller devices, is an increasingly common news topic. An intruder can break into a consumer's wireless computer or network in a way that is similar to that of most computers with Internet access – for example, through an e-mail virus. Moreover, there may be additional ways for hackers and others to obtain data from mobile devices (*e.g*. Bluetooth, Radio Frequency Identification ("RFID") chip) and infect mobile devices (*e.g*. through application downloads). Although spam and malware are currently not as prevalent on mobile devices as on computers, as the use and value of mobile transactions grows, so will interest in obtaining personal and financial data and using mobile devices for spam scams, identity theft, etc.

Moreover, as discussed above, the use of mobile devices to make payments is becoming more common. In some countries, mobile payments are generally conducted via SMS, or text messaging, while in other countries, mobile devices are being equipped with RFID chips that are able to transmit payment information to reading devices simply by waving their mobile device in front of a scanner in order to make a payment. This may open up new security risks.

The *E-commerce Guidelines* (Part II, Section II "Privacy") apply to this situation to the extent that they call for business-to-consumer e-commerce to be conducted in accordance with recognised privacy and security principles set out respectively in the *1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data* ("the Privacy Guidelines"), the *2002 OECD Guidelines for the Security of Information Systems and Networks*, and taking into account the *1998 OECD Ministerial Declaration on Protection of Privacy on Global Networks*. There may, however, be a need for additional measures. It might be beneficial for participants in mobile commerce to:

- Ensure that consumers are informed about the potential security and privacy challenges they may face in m-commerce and the available measures which can be used to limit the risks.
- Encourage the development of security precautions and built-in security features.
- Encourage mobile operators to implement data security policies and measures to prevent unauthorised transactions and data breaches; and
- Provide consumers with timely and effective methods of redress when their data is compromised and/or they suffer financial loss.

Location-based privacy and security issues

Unauthorised tracking

A mobile operator uses a Global Positioning System ("GPS") or triangulation (from signals generated from the device) to locate mobile users. The company sells the location and subscriber information to marketing companies for use in sending tailored advertisements or notices to the mobile subscriber. The mobile subscriber has not understood nor has she authorised transfer of such personal information. She might be charged for the notices (e.g. text messages about nearby sales or Internet time for pop-up messages). She is disturbed by the tracking and concerned that the information could be picked up (stolen or bought) by criminals.

The above example illustrates challenges raised by location-based information tracking. At issue is the lack of a process to safeguard information and, as in the hypothetical example discussed earlier in relation to the protection of children (*Keeping track*), the lack of a mechanism to disable tracking for non-emergency purposes.

The need for protections to safeguard location-based information might be addressed by the principle in Section VII, Part II of the *E-commerce Guidelines* that business-to-consumer electronic commerce should be conducted in accordance with recognised privacy principles set out in the *1980 Privacy Guidelines* (Part II, 7-10) and taking into account the *1998 OECD Ministerial Declaration on Protection of Privacy on Global Networks*.

It would be beneficial for businesses to:

- Provide consumers with clear disclosures about any location information that is being collected and the intended use of such information.
- Provide consumers with the opportunity to limit the sharing of data with third parties (except in emergency situations), and to revise their decisions about whom such data can be shared with.

In addition, companies that collect location data should take appropriate steps to safeguard such information, particularly when the data are sensitive or can be traced back to a particular individual.

Appendix I.1:
PROTECTING MINORS:
LAWS AND SELF-REGULATORY SCHEMES IN SOME OECD COUNTRIES

Access to adult content

Actions have been taken in a number of countries to address the challenges that mobile phones present. In Australia, Denmark, Germany, Japan, Korea, Norway, the United Kingdom and the United States, for example, mobile operators have developed voluntary codes of conduct to restrict access to adult content. In the United States, some mobile operators have adopted voluntary content classifications and Internet access controls to limit adult content access and enable parents to control it (see www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36). Under these guidelines, participating carriers currently block all adult-oriented content websites and would restrict access to such content through a portal only accessible to consumers at least 18 years of age or when authorised by a parent or guardian. Moreover, the Children's Internet Protection Act ("CIPA") requires schools and libraries participating in the E-rate program – a program that makes certain technology more affordable for eligible schools and libraries – to certify that they have an Internet safety policy including technology protection measures to block or filter Internet access to material that is obscene, contains child pornography, or is harmful to minors.

In addition, the Mobile Marketing Association ("MMA"), an international group that has guidelines in both Europe and the United States, has recently revised its US best practices guidelines for marketing to youth under the age of 13 (see www.mmaglobal.com/bestpractices.pdf). The guidelines, for example, provide that for audio and visual disclosures, participants must be at least 18 or have parental permission. Likewise, in February 2007, leading European mobile operators agreed on a European Framework on Safer Mobile Use by Younger Teenagers and Children (see http://ec.europa.eu/information_society). Under this framework, mobile operators support the development of awareness raising campaigns for parents and children; classification of commercial content (restricted adult content versus generally accessible content); and the development of age verification procedures.

Protecting children's personal data

Countries could explore adapting existing laws and rules protecting children on line to the mobile environment. For example, in the United States, federal law restricts the collection, use, or disclosure of personally identifiable information from and about children under the age of 13 in online services. This includes notification about privacy policies; verification of parental consent for collecting personal

information from children (with limited exceptions); parental review and deletion of personal information from their children; and requirements for procedures to protect the security of the data.

Overconsumption of services offered through mobile phones

Some countries have gone much further, placing greater responsibility on mobile operators. In Finland, the Consumer Complaints Board has established the responsibility of service providers in a case involving TV games played with text messages. The mobile operator was found to have received unfounded gains. The fact that a parent had allowed his/her child to use the parent's telephone did not in itself permit the child to legally enter into a commercial transaction such as the TV game in question. Under the decision, the consumer was eligible for a refund.

Marketing targeting children

The *E-commerce Guidelines* recommend that businesses should take special care in advertising or marketing that is targeted at children as they may not have the capacity to fully understand the information presented to them. Similarly, the MMA guidelines *(*para. 4.0), state that offering "programs that engage children in the promotion/consumption of digital content of any type imposes important ethical considerations, responsibility, and sensitivity that all industry participants are expected to uphold." While some countries have laws or regulations limiting such marketing, few have provisions pertaining specifically to mobile commerce. One exception is the United Kingdom, where junk food advertisement targeting children through mobile phones has been banned.

The US version of the MMA guidelines for short and multimedia wireless messages directed to children under 13 (see para. 4.0) call for all wireless industry participants to disclose that the service is a premium charge (when applicable) in all advertising in audio and visual; the actual cost of the charge and; if applicable, the fact that the standard messaging fees also apply. The guidelines also state that the word "free" may not be used unless there are no fees or charges associated with the service.

In Finland, the Guardianship Services Act provides that minors may only perform transactions which are usual for their age and have little significance. Under the Finnish Communications *Market Act*, the Finnish Communications Regulatory Authority defines *barring categories for telecommunications*. Subscribers, for example parents, can themselves determine the types of additional-cost services they want to block calling or texting to. Barring a certain category of services blocks all services which belong to the category in question. The Consumer Ombudsman has also negotiated some improvements in relation to the status of minors as subscribers of mobile services and has co-operated with businesses in that regard. Attention has been drawn to system maintainers' own responsibility for the system they use and compliance with already existing legislation. The Consumer Ombudsman has also drawn mobile operators' attention to their responsibility as the billing entity, including handling claims and compensation, as appropriate.

Unauthorised use of mobile phones

In Finland, the issue of the identification of the contracting party has been examined. The Ministry of Justice has, for example, set up a working group to draft a Government bill amending legislation on SMS instant loans. Consumer identification is currently only based on information about mobile subscriptions and social security numbers. The working group will consider whether there should be a statutory obligation for credit providers to identify customers in a more reliable way.

Privacy considerations

The Finnish *Act on the Protection of Privacy in Electronic Communications* requires that permission must be obtained from consumers before electronic direct marketing can be sent to them. The Data Protection Ombudsman and the Consumer Agency/Consumer Ombudsman have for example developed guidelines in relation to the so-called "tell a friend" marketing practice, which requires permission in advance from the recipient ("tell a friend" marketing refers to consumers forwarding product tips, introductory offers, contest invitations and other marketing messages to people they know by e-mail or text message).

The Finnish Act on the Protection of Privacy in Electronic Communications covers also confidentiality of identification and location data. This includes limits to the processing of identification data, such as processing for marketing purposes, and limits to the processing and disclosure of location data. It also covers the requirement of service-specific consent of the party to be located. In the case of minors under the age of 15, the guardian is responsible for deciding on the processing of location data.

In the United States, a carrier's ability to transmit users' location information to third parties is limited by statutory rules regarding the use of Customer Proprietary Network Information ("CPNI"*).* Specifically, Section 222 of the US Federal Communications Act prohibits the disclosure or use of wireless location information, obtained by a carrier by virtue of its provision of telecommunications services, without the express prior authorisation of the customer, except in specified emergency situations to respond to a wireless user's emergency call or in the transmission of automatic crash data. Further, the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN SPAM") Act prohibits mobile service commercial messages from being sent directly to wireless devices through the Internet without a subscriber's express prior authorisation. Additionally, the United States' Telephone Consumer Protection Act ("TCPA") prohibits any call using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number, including both voice calls and text messaging calls to wireless phone numbers.

Appendix I.2:
OECD INSTRUMENTS ADDRESSING MOBILE COMMERCE ISSUES

Consumer protection instruments

- 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.
- *2003 OECD Guidelines for the Consumer Protection against Fraudulent and Deceptive Commercial Practices Across Borders* (OECD, 2003), which establish a framework to combat all sorts of offline and online fraudulent activities at both domestic and international levels.
- *2007 OECD Recommendation on Consumer Dispute Resolution and Redress* (OECD, 2007c), which aims at providing consumers with effective mechanisms to settle their claims and obtain redress, whether at domestic or cross-border levels.
- 2008 OECD Policy Guidance on Online Identity Theft.

Security, privacy, and anti-spam instruments

- *2002 OECD Guidelines for the Security of Information Systems and Networks* (OECD, 2002), which set out principles to ensure consistent domestic approaches in addressing security risks in a globally interconnected society.
- OECD (2007d), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.
- *1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 1980), which contain principles on the collection and processing of personal information.
- *2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (OECD, 2007e), which calls on member country authorities to co-operate with foreign authorities and assist each other in the enforcement of privacy laws.
- *2006 OECD Anti-Spam Toolkit of Recommended Policies and Measures*, which aims at facilitating international co-operation in the fight against spam and provides a set of recommendations to put in place complementary policies in the enforcement of anti-spam initiatives among OECD member countries.

BIBLIOGRAPHY

EC (European Commission) (2006), *Special Eurobarometer Safer Internet*, May 2006, http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.

EC (2007), *12th EU Implementation report on European Electronic Communications Regulation and Markets*, COM(2007)155, 29 March 2007, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/12threport/com_2007_155_en.pdf.

ITU (International Telecommunications Union) (2004), *Mobile phones and youth, a look at the US student market*, February 2004, www.itu.int/osg/spu/ni/futuremobile/Youth.pdf.

OECD (Organisation for Economic Co-operation and Development) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD, Paris, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OECD (1999), *Guidelines for Consumer Protection in the context of Electronic Commerce*, OECD, Paris, www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

OECD (2002), *Guidelines for the Security of Information Systems and Networks*, OECD, Paris.

OECD (2003), *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/crossborderfraud.

OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, OECD, Paris, www.oecd-antispam.org/.

OECD (2007a), *Mobile Commerce*, DSTI/CP(2006)7/FINAL, www.oecd.org/sti/consumer-policy.

OECD (2007b), *OECD Communications Outlook 2007*, OECD, Paris, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF.

OECD (2007c), *Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, www.oecd.org/dataoecd/43/50/38960101.pdf.

OECD (2007d), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

OECD (2007e), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, www.oecd.org/dataoecd/43/28/38770483.pdf.