September/2002

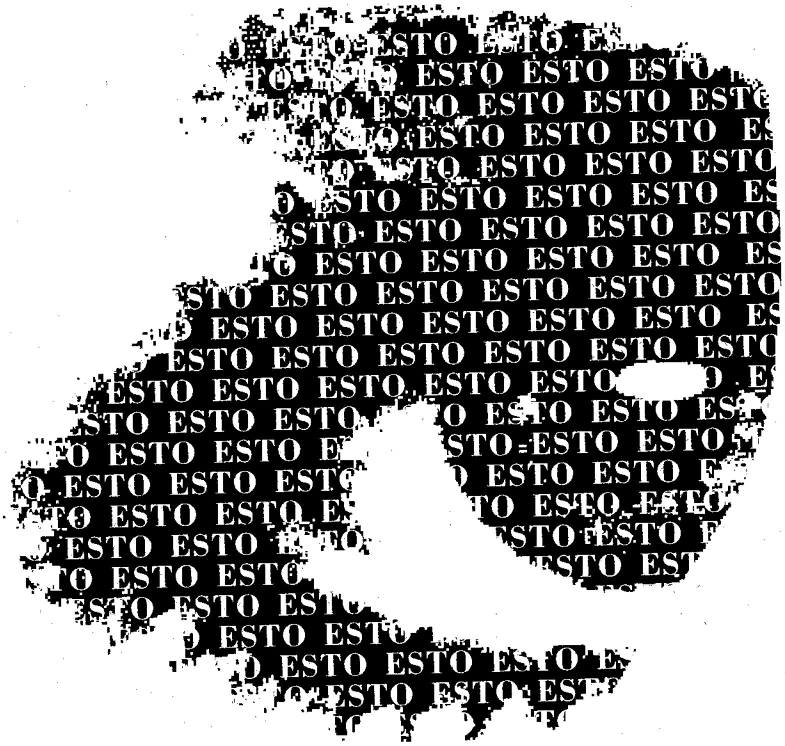
67

ISSN: 1025-9384

5 EURO ΕΥΡΩ

# The IPTS REPORT

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)
AND ISSUED IN COOPERATION WITH THE EUROPEAN S&T OBSERVATORY NETWORK



## SPECIAL ISSUE: IDENTITY AND PRIVACY

EUROPEAN COMMISSION
Joint Research Centre

ENGLISH VERSION

THE IPTS REPORT

67

SEPTEMBER 2002

# CONTENTS

## Special Issue: Identity and Privacy

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)
And issued in Cooperation with
the European S&T Observatory Network

**PUBLISHED BY THE EUROPEAN COMMISSION**
Joint Research Centre
ISSN: 1025-9384
Catalogue Number LF-AA-02-067-EN-C
DEPOT LEGAL: SE-1937-95

**DIRECTOR**
Jean-Marie Cadiou

**EXECUTIVE EDITOR**
Dimitris Kyriakou

**PRODUCTION**
CINDOC-CSIC/BGS

**PRINT**
Graesal

**TRANSLATION**
CINDOC-CSIC/BGS

**THE IPTS REPORT**
is published in the first week of every month, except for the months of January and August. It is edited in English and is currently available at a price of 50 euro per year, in four languages: English, French, German and Spanish.

**SUBSCRIPTIONS**
For a subscription to The IPTS Report, or to amend an existing subscription, please write with full details to:
The IPTS Report Secretariat
IPTS, JRC Sevilla
Edificio Expo-WTC
C/ Inca Garcilaso, s/n
E-41092 Sevilla, Spain
Tel: +34-95-448 82 97
Fax: +34-95-448 82 93
E-mail: ipts_secr@jrc.es
Web address: www.jrc.es/iptsreport/subscribe.html

vehicle of the cyber-citizen in this new digital environment. The European Union, is today working out how to wed sustainable development with increased mobility. For this strategy, the management of identity will constitute one of the first challenges for this mobile Europe in order to facilitate cyber navigation and social interactions between European citizens in the Information Society. These identity management tools, which could be a piece of software, an intelligent agent or even a chip embedded in the body will have to respect the user's privacy and security, and they will also have to facilitate the application of laws in these new digital territories. In other words, the balance between individual rights and duties, which have evolved out of an extensive socio-cultural process, will have to be preserved in the Information Society. Therefore, there is a clear need to assess the implications for the regulatory framework.

The main objective of this Special Issue of *The IPTS Report* is to explore in a prospective way the many impacts of emerging technologies on the future of Identity and Privacy, as well as assessing the different policy options in this field.

In the first article, Esther Dyson explores the evolution of the concept of identity and underlines the emerging issues which will have to be addressed in order to create a safer and more trustworthy Information society.

Then, in the second article, Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen set out to define the most important requirements for the building of identity management systems, able to simultaneously enhance the user privacy and meet security requirements. Indeed, today's existing identity management systems have no, or limited, privacy goals or functionality, or may even threaten users' privacy if they store and process personal information without appropriate protection measures. Therefore new systems have to be designed and built into the infrastructure.

In the third article, Laurent Beslay and Yves Punie develop the concept of the Virtual Residence, which could contribute to a better perception and consideration of an individual's personal digital territory and could help to tackle the blurring boundaries of what is public and private in the online world.

In the fourth article, fuelling the prospective exercise on Identity and Privacy, Thierry Nabeth and Claudia Roda analyse the potential role of software agents in the evolution of the identity concept and underline new issues generated by this technology.

Finally, in the last article, Kevin Warwick addresses the potential impact of cyborg technology on the identity-related issues raised by enhancing human abilities through the use of biomedical implants.

## Contacts

Laurent Beslay, IPTS
Tel.: +34 95 448 82 06, fax: +34 95 448 82 08, e-mail: **laurent.beslay@jrc.es**
Jean-Claude Burgelman, IPTS
Tel.: +34 95 448 84 96, fax: +34 95 448 82 08, e-mail: **Jean-Claude.Burgelman@jrc.es**
Ioannis Maghiros, IPTS
Tel: +34 95 448 82 81, fax: +34 95 448 83 39, e-mail: **ioannis.maghiros@jrc.es**

Cell-phone operators and many software vendors, especially in Europe, want to focus your identity on your cell phone –a device you always carry with you, and with which you already have a billing relationship. What could be simpler?

Just as it seems everyone –from banks to brokerages to insurance companies to financial advisors– wants to manage your money for you, so will everyone want to manage your identity for you!

What do these services allow you to do? Plenty. For instance, they let you manage and maintain passwords, membership numbers, pin numbers, e-mail addresses and the like. If you're trusting and have given permission (we hope!), a "single sign-on" will allow you to sign on once and then the service automatically hands over the correct passwords, credit information or whatever to the sites you visit. Some services can help you specify which information you want to reveal to whom, and to transfer identity information easily to other people's identity services, among other things. Again, it's similar to what happens now with money: The data is yours, but the institution manages it for you.

## Emerging Issues on Identity in the Information Society

The question of identity is not a new issue. For a long time, companies have been developing a variety of systems in this area – everything from passwords and customer databases to cookies that sit invisibly on your computer and potentially send or point to data about you and possibly your online activities to the Websites you visit. They're creating a world of tremendous convenience – those cookies let Orbitz know who users are so they don't need to reenter their data – but the real new issue is the need to become more transparent so that people will trust it and adopt it massively.

The first rule of identity management is that it should start from the individual. There is in fact a hierarchy of identities which begins with Tier 1 – the inalienable identity of the individual. There is a political underpinning to this that some people may find objectionable, namely that there should be only one identity to an individual. . That's what law-enforcement wants, and so do most institutions (it makes life simpler!). But a lot of people like experimenting with multiple identities. Some are content to do so in the context of different facets of the same identity – church-goer on Sunday, disco dancer on Friday – while others, for reasons that may or may not be legitimate–, like to avoid being directly associated with all their actions or history by assuming another identity (or at least anonymity). More and more, people in our society are feeling comfortable with multiple IDs. In the last PC Forum, not a very representative group of people, of course, about half of them had more than one e-mail address or online name. Some had five or more. This first tier of identity establishes a clear contradictory situation between the wish of public organization to deliver a single and unique identity and the wish of the user to develop and manage multiple identity.

The second tier of identity is information in the context of other institutions – everything from your address(es), and your employee number (and all your records), to your passport, your accounts with various merchants, and your memberships in various organizations. This Tier 2 identity is the one with the most data, and the one where there are all the privacy concerns. Most people have multiple Tier 2 identities. It would be convenient in many ways for them to be better linked. It's the linking of Tier 2 data that governments want also in order to detect terrorists – in theory, at least. Certainly there are patterns that can raise suspicion, but there is so much data to mine that the correlations are generally discovered after the fact. Everyone knows by now that buying a one-

*The focus for new business opportunities may be shifting from emphasis on offering services to help people manage their money to services to help people manage their online identity*

*Identity management needs to start out from the individual. Here the authorities may require a single, unique identity, whereas individuals may prefer multiple identities for use in different contexts* and its counterpart, security. But people will also have tools to deal with other people's and organizations' identities, determining everything from the people they will talk to, to the companies they will do business with. They may not want to see items ranked below 4 by some opinion survey, or they may not want to hear from people ranked below 6 in their own address book. A lot of technology and market experts will be spending a lot of time and money to promote technology that manages identity. The winners in this game will be the ones who understand that people want to control their own information, without being confused by the tools that help them do it. Indeed, software developers and policy-makers will have first to reconcile often contradictory expectations on identity management held by individuals on one hand and by organizations on the other.

**Keywords**

digital identity, privacy, authentication, certification, security, authorization

**Contacts**

Esther Dyson, Chairman, EDventure Holdings

Tel.: +1 (212) 924 88 00, fax: +1 (212) 924 02 40, e-mail: **edyson@edventure.com**

Laurent Beslay, IPTS

Tel.: +34 95 448 82 06, fax: +34 95 448 82 08, e-mail: **laurent.beslay@jrc.es**

**About the author**

**Esther Dyson** is an investor and commentator focusing on emerging information technologies, emerging markets and emerging companies. She is a board member of several "emerged" companies, including Manugistics and WPP Group, and was founding chairman of ICANN, the Internet Corporation for Assigned Names and Numbers, 1998-2000. In 1997, she wrote a book on the impact of the Internet on individuals' lives, "Release 2.0: A design for living in the digital age." . Dyson is chairman of EDventure Holdings, which publishes a monthly computer-industry newsletter, Release 1.0, and sponsors the PC Forum conference in the US and EDventure's High-Tech Forum in Europe.

In the Information Society users are likely to define and handle their digital identities and roles in a similar way, and assert and enforce their right to privacy. In the digital world, this is a real challenge: Technology trends like the dissemination of (mobile) personal devices, ubiquitous access and computing, together with the e-transformation of business, government, and work processes, raise usability, security, and management issues which often are (but need not be) addressed by increasing the degree of linking, centralization, and logging of information. In the digital world, there is not only the possibility of creating new identities for oneself, but every user leaves data trails while using digital applications or services. Most people are not aware of how much the data they leave says about them and have no way of effectively controlling this data leakage. On the other hand, there is no guarantee that data in digital networks is authentic. In particular, fake identities can be created, and even identities of existing people can be "borrowed" – meanwhile identity theft is a fast growing problem (**http://www.identitytheft.org**). Thus today's digital world lacks both privacy and authenticity.

In the Information Society envisioned, privacy-enhancing identity management systems (IMSs) enable us to perform our roles, use our identities, and retain our privacy in society in the same way we have been allowed to up until now. Our personal environment and devices, rather than being just huge data repositories of our on-line actions, passwords, etc. also help us to keep track of, and protect the privacy of, our digital identities including their rights and obligations; and to choose when and to whom to give personal information. Communication networks allow us to hide our "coordinates" such as physical location, network or e-mail addresses and protect them from being misused, while still allowing network administrators to manage their networks securely. We can use electronic equivalents of every-day items such as library, gym or bus passes, phone books, or cash, without enabling extensive tracking and profiling of our behaviour across the different areas of our lives.

Privacy-enhancing IM combines privacy with authenticity. It requires technologies that allow users to control the release of personal information and to control the linkability of different occurrences of this information in different contexts (Pfitzmann/Köhntopp 2001) by acting under pseudonyms or anonymously. Authenticity can be achieved in combination with varying degrees of anonymity (Chaum 1984, Clarke 1999, Pfitzmann/Waidner/Pfitzmann 2000).

*In the digital world, most people are not aware of how much the data they leave says about them and have no way of effectively controlling this data leakage*

## Approaches to Identity Management

Approaches to IM mainly differ in terms of the location where user profiles are stored and processed (user's side only / user's and server side / server side only) and in the provision of authentication mechanisms and additional security and privacy functionality. Having in mind the design of a comprehensive privacy-enhancing IMS, various shortcomings of the existing approaches can be enumerated:

- **Lacking support for users' sovereignty:**
  In most cases users cannot choose where and how their personal data are managed: They have to trust central IM providers who have full access to their data.
- **Limited privacy functions:**
  Few systems help the users' awareness or assertion of their right to privacy.
- **No pseudonymous authentication:**
  Currently, the state of the art in pseudonymous and anonymous credential systems (cf. Camenisch/Lysyanskaya 2001) allows for provably secure implementations of authenticated anonymous transactions and user-controlled release of certified attributes. In particular, they allow each user to use a cre-

*Privacy-enhancing IM combines privacy with authenticity. It requires technologies that allow users to control the release of personal information and to control the linkability of different occurrences of this information in different contexts*

Legal or organizational measures alone are not sufficient to help users with their IM. The lack of privacy in existing systems highlights the need for new privacy-enhancing technological solutions, taking into account existing legal systems and possible business models. There is also a need for actions to educate and train users in privacy and IMSs.

Moreover, privacy-enhancing IM requires new technologies and third party services to be provided as part of an IM infrastructure (see below). Therefore, a comprehensive approach to IM is needed, which is not offered by any of the existing systems discussed above.

## Design of an IMS: Requirements and Functionality

A privacy-enhancing IMS makes the user aware of and gives him/her control over the flow of personal data. To show the user that flow of data, the IMS must give him or her meaningful history and context representations. History information includes the extent, nature, and linkability of data released in the past; context information may include additional information, e.g., specific tags to express when actions have to be linked or what properties a new pseudonym should have, and can be provided by communication partners, third parties such as a privacy information service or even the Internet community.

In order to give the user control over the flow of personal data, the IMS supports each user in deciding and enforcing which identifiable or pseudonymous personal data he or she releases. It enables the user to minimize the dissemination of personal data and to determine the degree of linkability of his data by choosing which pseudonyms are used with which properties, and whether to re-use pseudonyms or to generate new ones.

It gives the user the mechanisms and interfaces to implement his privacy rights, e.g., to get information from a server about what personal data that server holds about him or her, to access these data, to correct or remove these data, or to grant or revoke consent.

Usability and a good user interface are essential and may include support by on-line privacy information services providing information about security and privacy risks with respect to the IMSs deployed.

The user should be able to access his IM tool from a variety of devices (e.g., a mobile phone or PDA) and locations. Also, less capable devices should provide a usable interface and at least minimal functionality.

Ideally, the user's IMS is located in the user's trusted environment. For various reasons (e.g., reachability of the system when using different devices, convenient replication, or back-up services), users may want to outsource all or part of their IMS to a provider. The user should be able to select the provider.

Privacy and identity management should not hinder the enforcement of security measures or the effectiveness of intrusion detection systems. In many cases there need not be a contradiction between law enforcement requirements and full privacy: appropriate design of applications can prevent misuse so that the user's anonymity need not be reversible (Pfitzmann/Waidner/Pfitzmann 2000). When designing IMSs and deploying anonymous and unlinkable transactions, systems and tools enforcing security may have to be reconfigured or adapted in order to deal with these varying degrees of anonymity or pseudonym properties such as restricting users to a fixed number of pseudonyms per subject, transferability to other subjects, possibility and frequency of pseudonym

*The lack of privacy in existing systems highlights the need for new privacy-enhancing technological solutions, taking into account existing legal systems and possible business models*

*Privacy and identity management should not hinder the enforcement of security measures or the effectiveness of intrusion detection systems. In many cases there need not be a contradiction between law enforcement requirements and full privacy* the exchange of goods without revealing additional personal data. Unlinkability of the 'who (buys)' and the 'what (is bought)' in a partially on-line purchase may be achieved by applying 'separation of knowledge' between payment and delivery services (i.e. neither the party handling payment nor the party handling delivery has the full details of the user). Also, the communication infrastructure needs to support basic security and privacy (e.g., network layer authentication, confidentiality, and possibly anonymity) as well as robustness. The principles of distribution of trust and separation of knowledge and power should be applied in the design of these third party services, in order to limit the threat of information sharing between third parties. Also, it should be possible for users to enforce their trust preferences.

The user's IDM acts as a central gateway for all communication between different applications, like browsing the web, buying in Internet shops, or carrying out administrative tasks with governmental authorities. By acting as a central gateway, it allows the user to be aware of the flow of personal data, and to control the release of data, in accordance with the specified requirements.

As discussed above, distributed implementation of the user's IDM is possible. For example, the graphical user interface (GUI) can be implemented on (less capable) mobile devices while the other modules are located at a more powerful fixed station, using secure communication to the external GUI. Also, part of the user's IDM may be located at an IDM proxy provider.

The IDM tools at the application services are needed primarily to handle anonymous or pseudonymous requests, and especially pseudonymous authentication of users. It also provides the user with context information about the transaction, e.g. information about pseudonym properties needed.

To provide maximum interoperability, common standards for protocols and interfaces need to be defined, so as to permit a combination with existing systems to enhance their privacy functionality.

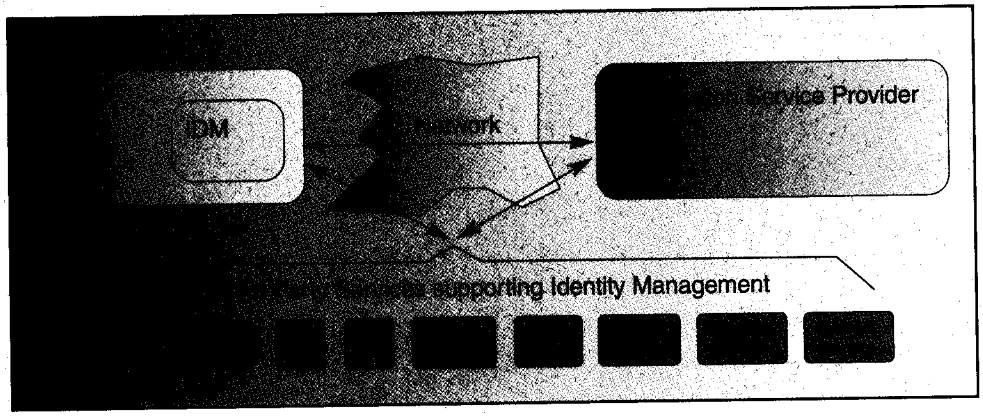
## Outlook

Privacy-enhancing IM is necessary to preserve and update the concept of privacy for the Information Society. Our vision of privacy-enhancing IM can only be fully achieved if we design applications, middleware, and communication infrastructures so that they support the IM architecture and technologies proposed. Of course, its implementation will happen using an evolutionary approach, as technologies supporting it will be introduced gradually and will coexist with today's systems.

*The user's IDM acts as a central gateway for all communication between different applications, like browsing the web, buying in Internet shops, or carrying out administrative tasks with governmental authorities*

*Privacy-enhancing IM is necessary to preserve and update the concept of privacy for the Information Society*

***Figure 1. Basic Components of an IMS***



## Drivers for Privacy-Enhancing IMSs

We see three main drivers for developing privacy-enhancing IMSs, each contributing their specific interests:

- privacy law (EU Directive 1995), enforced by the government, also taking into account the requirements of law enforcement agencies;
- users who demand such systems to achieve better privacy;
- economic considerations, calling for the creation of new IMS business models or adapting them to enable lasting customer relationships without expensive processing of personal data with all its privacy obligations.

The issue of whether these driving forces are sufficient to develop good privacy-enhancing IMSs, and the need for users to be appropriately informed and educated, are no doubt of interest to policy-makers. Moreover, any regulations in this field need to be specific and up-to-date with privacy-enhancing technologies, such that they provide the correct incentives for enterprises to create and put in place the IMS-supportive business models.

There is a need for an interdisciplinary discussion on the future of identity and privacy (Bogdanowicz/Beslay 2001), which should lead the way to comprehensive privacy-enhancing IMSs. Technological know-how is necessary for this discussion: The digital world works differently from the physical world; it may threaten privacy, but it also provides the means to cope with such threats or even shows opportunities for better privacy protection than before.

**Keywords**

privacy, identity management, security, trust

## References

- Berthold, O., Federrath, H., and Köhntopp, M. *Anonymity and Unobservability in the Internet*", Workshop on Freedom and Privacy by Design. In Proceedings of the Tenth Conference on Computers, Freedom & Privacy, CFP 2000: Challenging the Assumptions, Toronto/Canada, April 4-7, 2000. ACM, New York 2000. 57-65.
- Bogdanowicz, M., and Beslay, L., *Cyber-Security and the Future of Identity.* In The IPTS Report No. 57, JRC Seville, September 2001. **http://www.jrc.es/pages/iptsreport/vol57/english/ICT4E576.htm**
- Camenisch, J. and Lysyanskaya, A. *Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation.* In B. Pfitzmann (Ed.), Advances in Cryptology – EUROCRYPT 2001. LNCS 2045. Springer Verlag, 2001. 93-118.
- Clauß, S. and Köhntopp, M. *Identity Management and Its Support of Multilateral Security.* In Computer Networks 37 (2001). Special Issue on Electronic Business Systems. Elsevier, North-Holland 2001. 205-219. **http://www.elsevier.com/gej-ng/10/15/22/67/33/34/article.pdf**
- Chaum, D. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Communications of the ACM, 24(2) February 1981.
- Chaum, D. *Security without identification: Transaction systems to make big brother obsolete.* Communications of the ACM, 28(10) October 1985, 1030-1044. **http://www.chaum.com/articles/Security_Wthout_Identification.htm**
- Clarke, R. *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice.* In S. Fischer-Hübner, G. Quirchmayr, L. Yngström (Eds.), User Identification & Privacy Protection:

## About the authors

**Sebastian Clauß** has a diploma degree in informatics from Dresden University of Technology, Germany, where he studied from 1994 to 2000 and where he is currently engaged in research into data security and privacy. His research interests and published work focus in particular on technologies for anonymity and identity management.

**Andreas Pfitzmann** is a professor of computer science at Dresden University of Technology. His research interests include privacy and multilateral security, mainly in communication networks, mobile computing, and distributed applications. He has authored or coauthored about 70 papers in these fields. He received diploma and doctoral degrees in computer science from the University of Karlsruhe. He is a member of ACM, IEEE, and GI, where he serves as chairman of the Special Interest Group on Dependable IT-Systems.

# The Virtual Residence: Identity, Privacy and Security

Laurent Beslay and Yves Punie, *IPTS*

**Issue:** In the physical world, domicile and residence are carefully developed and recognized concepts. A comparable level of sophistication is needed for people to feel acceptance and trust towards their online activities. The concept of "Virtual Residence" could help to tackle concerns of identity, privacy and security for peoples' online activities. It could contribute to a better perception and consideration of ones' personal digital territory and could help to tackle the blurring boundaries of what is public and private in the online world.

**Relevance:** People, families and homes are increasingly being connected to the Internet. Living online will be an important constituent of our everyday lives in the future e-Society. This raises key policy concerns in relation to identity, privacy and security.

## Life online as a new private space

According to MIT professor Nicholas Negroponte, the Information Society is deepening and widening as each new generation becomes more digitized than the preceding one. More and more personal information will, as a result, be disclosed in the virtual world. This concerns not only basic personal identification data such as age, sex and location[1] but also personal calendar information, working documents, family albums (pictures, video, chat) and medical and financial records. This information can be stored in personal databases, personal and/or family websites or even in community websites hosted by private companies or other institutions. As such, people are creating a new kind of online private space.

For people to feel at home in their online private space (at least) three major challenges have to be faced. The space should represent people's multiple identities (legally and socially), respect their privacy and establish an acceptable level of security. These challenges are related to the fundamental but complex interrelationship between what constitutes the private and the public.

In the physical world, legal rules and socio-cultural norms and habits constitute the guidelines

*As the Information Society develops and each successive generation becomes more digitized, ever more data will be disclosed in the virtual world*

*For people to feel at home in an online private space it needs to be able to represent their multiple identities, respect their privacy and establish an acceptable level of security*

*The views expressed here are the author's and do not necessarily reflect those of the European Commission.*

Please return the form by post to:

**The Evaluation Partnership**
**11 Normandy Gardens**
**Horsham**
**West Sussex**
**RH12 1AS**
**United Kingdom**

## SUBSCRIBER BACKGROUND INFORMATION

1. In which year did you first start reading the IPTS Report? □□□□

2. Which of the following best describes how you first discovered the IPTS Report? (Choose one)

□ Through my organisation
□ At a conference
□ Through a colleague or friend
□ Through the Internet
□ Other (please specify) ____________

3. Which of the following best describes your background or expertise? (Choose one)

□ Agriculture/Food
□ Business management
□ Economics
□ Energy
□ Environment
□ ICT
□ Legal
□ Life sciences
□ Mathematical sciences
□ Physical sciences
□ Research and development
□ Social sciences
□ Transport
□ Urban/Regional planning
□ Other (please specify) ____________

4. Which of the following best describes your place of employment? (Choose one)

□ ESTO member organisation
□ European Union Institution
□ Press or journalism
□ Private sector
□ Public administration of an EU member state
□ Public administr. of a non-EU member state
□ Research centre or laboratory
□ University or higher education
□ Other associations or NGOs
□ Other (please specify) ____________

5. Which of the following best describes your work within your organisation? (Choose one)

□ Academic research
□ Communication
□ Engineering
□ Policy advice
□ Policy implementation
□ Policy making
□ Private sector management
□ Private sector strategy
□ Research
□ Teaching
□ Other (please specify) ____________

## SUBSCRIBER FEED-BACK ON THE PUBLICATION

6. Which of the following are your reasons for reading the IPTS Report? (Choose those applicable)

□ Alerting me to the socio-economic impact of technology
□ Alerting me to technological developments
□ Anticipating policy needs
□ Understanding policy issues
□ Other (please specify) ____________ ____________

7. How do you use the information provided in the IPTS Report? (Choose those applicable)

□ For activities related to projects in my work.
□ For background research.
□ For developing contacts and networking.
□ For increasing my knowledge of policy in general
□ For preparing meetings and presentations.
□ Other (please specify) ____________

8. How easy is it for you to identify relevant articles and extract pertinent information from the Review?

□ Very easy □ Easy □ Difficult □ Very difficult

9. How would you rate the value of your time spent reading the IPTS Report? (Choose one).

□ Very high □ High □ Low □ Very low

10. Besides yourself, approximately how many others read your copy of the Report? (Choose one)

□ Nobody □ 1-4 □ 5-9 □ 10 or more □ Don't know

11. What do you do with your old copies of the Report? (Choose one)

□ Keep them myself □ Pass them to others □ Place them in a library □ Throw them away □ Other

12. Are you aware that the Report is available on the Internet? □ Yes □ No

13. Have you ever accessed the Report on the Internet? □ Yes □ No

14. Which version do you prefer? □ Printed version □ Internet version □ Both

15. Would you like more standard editions, more themed editions, or same balance as now? (Choose one)

□ More standard editions □ More themed editions □ Maintain the existing balance

16. Would you like to see more technological information, more socio-economic impact information, or the same balance as now? (Choose one)

□ More technological information □ More policy-related socio-economic impact information □ Maintain existing balance

17. How often do you think the report should be published? (Presently there are 10 issues per year.)

□ More frequently □ The same frequency □ Less frequently

Similar to the legal and social extension of the domicile to a car that moves through physical space, it is possible to envisage online extensions of the virtual private space that encompass intelligent agents. The latter also move through time and space -albeit in the form of cyberspace- 'encapsulating' personal data in order to carry out requests for their real life counterparts. Some intelligent agents, for example in the area of online travel shopping, allow the user to compare the discounted airfares offered by major airlines and book them online[4]. In order to find the best flight ticket corresponding to the user specific criteria and to book it or even to buy it, this intelligent agent will have to "go" through numerous web sites with the user's personal data.

Another dimension of the public - private issue, with implications for identity, privacy and security, needs to be situated at the network level as is discussed in the next section.

## Critical domestic networks and Ambient Intelligence

The home of the future will become increasingly connected and will come to be seen as one of the 'nodes' in the network society.[5] The core infrastructure for the connected home will consist of so-called domestic networks. This may range from a narrow-band network for home automation purposes, through medium band networks for sharing computer data, to broadband networks for the distribution of audio-visual content. These networks may be both wired and wireless. Apart from the need for interoperability of these local networks, they will also be connected to external networks (Internet, fixed and mobile telecommunications, terrestrial, cable and satellite TV). The link between them is often referred to as a 'residential gateway'[6]

The future home is thus both internally and externally connected. A more all-encompassing vision of the communication structures within the connected home is increasingly being referred to as Ambient Intelligence (AmI). The ISTAG/IPTS report depicts a vision of the Information Society where the emphasis is on user-friendliness, efficient and distributed service support, user-empowerment, and support for human interactions. People are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and are living in an environment that is capable of recognizing and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way.[7] Humans, computers, intelligent agents and smart devices communicate with each other inside and outside the domestic network.

*The home of the future is likely to be increasingly connected: both internally through domestic networks and externally through broadband networks transmitting audio-visual content*

This raises a number of social and legal issues in relation to identity, privacy and security. The AmI system needs to know a lot of personal information in order to act in a personalized, intuitive and desirable way. It is aware of the identity and location of users and communicates this information to other persons, virtual agents, services, devices and objects. People need to be able to control, in one way or another, the nature and amount of personal information that is disclosed about them and need to be able to differentiate this according to the situation and the actors/systems they communicate with.[8] It is clear that peoples' privacy is at stake here and that these information exchanges need to be secured and managed.

*As systems become increasingly aware of the identity and location of users and able to communicate this information to other persons, virtual agents, services, devices and objects, privacy concerns inevitably arise*

When the web-connected oven downloads the latest recipe it will also reveal the eating habits of the inhabitants of the smart home. Even if this information could be seen as relatively innocent, its systematic collection may form part of the process of building an exhaustive and highly detailed profile of the user, without his or her knowing about it. One of the characteristics of ambient intelligence is exactly its seamless, invisible communication. The maintenance process of ambient intelligence systems will be driven by micro-pay-

*Architecture:* Experts[11] argue that the most feasible solution for the management of digital identity will be a decentralized system whereby people keep their personal data with them. The virtual residence could be a good place to store and manage personal information and multiple identities.

*Social norms:* The physical residence is protected by social norms and rules indicating, amongst other things, respect for other peoples' private affairs. These sophisticated social norms and rules are learned through institutions of socialization such as the family, school, work, etc. The virtual residence could acquire a comparable social status of one's 'online' private space.

Provided that the virtual residence is able to reflect multiple identities, to protect the privacy of these identities and to offer acceptable levels of security, it might facilitate the acceptance of new technologies at home, as briefly discussed in the final section of this article.

## The acceptance of the virtual residence

Research on use and acceptance of Information Society Technologies (ISTs) in the home highlights that people do not accept everything that is technologically available. People need resources (time and money) to buy and use ISTs and these resources are not evenly distributed in society. Moreover, they need to have the capabilities (education, skills, attitudes, language, etc.) to make use of ISTs. The latter should of course also be user-friendly, affordable and should provide users with functional and/or symbolic added value. [12]

It also has to be taken into account that use and acceptance of ISTs are negotiated within the existing social structures of the household. To understand this, Silverstone and others have developed the sociological concept of 'domestication'. This refers to a process of double change. First, an innovation has to be integrated into the structures, routines, rituals and dominant values of the members of the household. It has to be housetrained or 'domesticated'. Second, users and their everyday lives undergo changes when innovations are put to use. [13] In particular, when ISTs become taken for granted, in the sense that they are perceived as a natural and unobtrusive part of our everyday lives (e.g. TV, radio, phone), rather than enigmatic technical objects (e.g. video recorder, PC), they have the potential to change features of ordinary life.

*Many innovations have difficulties in reaching the stage where they are accepted to the point of becoming a natural and unobtrusive part of people's lives*

In order for the virtual residence to be accepted by people, socially and culturally determined patterns and structures of everyday life have to be recognized.[14] The smart home should be able to reflect the identities of its inhabitants in many different ways. For example, the preliminary results of a project called "Ambient Intelligence Homelab" recently launched by the electronics manufacturer Philips, comprising a fully equipped home in order to test prototype Ami Technologies and peoples' behaviour and reactions in a semi-real life environment, raised the issue of power relations in social interactions amongst family members.[15] Can intelligent agents take a position within these relations and who is to blame for unequal access within the family?

*If people are to accept the virtual residence it has to embrace socially and culturally determined patterns and structures of everyday life*

Trust, confidence and reliability are, among other factors, powerful enablers of domestication. If technologies do not deliver what they promise; if they do not react in ways they are supposed to react; and do not function when they are needed, then, it will be very difficult for them to become domesticated. This is also the case for the virtual residence. People need to feel at home in their virtual residence and technology design should take this into account.

*Trust, confidence and reliability are, amongst others, powerful enablers of "domestication" or the process whereby technologies become accepted into people's everyday lives*

The virtual residence will be involved in the continuous work of what sociologists refer to as

10. Art. 12 Universal Declaration of Human rights, and Art 8 European Convention for the protection of human rights and fundamental freedoms.

11. The future of identity in an e-Society. IPTS Workshop 10-11 December 2001 Seville, **http://cybersecurity.jrc.es**

12. See for an overview of ICT user research: Frissen, V. & Punie, Y. (2001), Present users, future homes. A theoretical perspective on acceptance and use of ICT in the home environment, Position Paper STB-01-30a for the Media@Home project, TNO, Delft, May 2001.

13. Silverstone, R. & Haddon, L. (1996). Design and the domestication of ICTs: technical change and everyday life. In: Mansell , R. & Silverstone, R., (eds.), *Communication by Design. The politics of Information and Communication Technologies.* Oxford: Oxford University Press, p.60.

14. Frissen, V. & Punie, Y. (2001), Ibid.

15. Aerts, E. (Ed.) (2002) Ambient Intelligence in HomeLab, Published by Philips Research for the occasion of the opening of the HomeLab on April 24, 2002, Philips Research, Eindhoven. **http://www.newscenter.philips.com**

16. Ontological security is a sociological term defined as a stable mental state derived from a sense of continuity and order in events.

## Contacts

Laurent Beslay, IPTS
Tel.: +34 95 448 82 06, fax: +34 95 448 82 08, e-mail: **laurent.beslay@jrc.es**
Yves Punie, IPTS
Tel.: +34 95 448 82 29, fax: +34 95 448 82 08, e-mail: **yves.punie@jrc.es**

## About the authors

**Laurent Beslay** has a post-master's degree (DESS) in Global Management of Risks and Crisis (University of Paris, la Sorbonne) for which he produced a report on the opportunities of a business intelligence unit for the Direction of Military Applications of the French atomic energy committee (CEA). He has a Master's degree in International Relations (Study Institute of International Relations), for which he produced a thesis on "The control of exports of dual-use goods and technologies ". He is currently working on a Ph.D. on "Electronic Surveillance: benefits and risks for the European Union", while at the IPTS-European Commission, ICT unit, where he is working on the future of identity project.

**Yves Punie** holds a Ph.D. in Social Sciences from the Free University of Brussels (VUB). His doctoral thesis was on the use and acceptance of ICTs in everyday life, also known as 'domestication of ICTs' (June 2000). Before joining the IPTS as a post-doc researcher in May 2001, he was a senior researcher at SMIT (Studies on Media, Information and Telecommunication, VUB). His main project is on the future of domestic new media technologies.

possibly making decisions on his or her behalf. An example of an agent of this kind would be an interactive on-line tutor which knows about the user's existing skills and qualifications, goals, and learning style and is able to use this knowledge to propose the most suitable learning strategy for this user. The agent would then go on to support the user in executing this strategy by selecting and delivering the most appropriate teaching materials, measuring the effectiveness of the learning process and even by giving the user encouragement. Other types of intelligent agents could help people at work, while shopping or help them choose entertainment.

The second category includes "social agents" that operate in digital "social spaces", such as "virtual community platforms", and whose role is to facilitate a process of social interaction. For instance, the function of some of these agents is to encourage group formation by clustering users with similar profiles and interest (often referred to as social or collaborative filtering[1]) and therefore connecting groups of people. The function of other social agents is to encourage knowledge exchange and collaboration, which they do by encouraging transparency. In practical terms, these agents track and display users' activity (such as who is active, who contributes, who is reliable) in digital "social spaces". A concrete example of this later category of agent can be found in eBay's auctioning system or the freelance marketplace eLance, which keeps track of the transaction history of all the participants (buyers and sellers), and which helps people to form an opinion about the reliability of establishing a transaction or a business relationship with another party.

### What are the implications for people's identity of using artificial agents?

Identity in this context refers to more than just "identity information" (such as a person's social security or tax number), rather it represents a more general concept which relates to the individual's development and his sense of belonging. Moreover, the next generation of artificial personal or social agents should not be confused with basic "anthropomorphic" wizards (such as the Microsoft agents) that provide help with certain simple and highly specific tasks. "Intelligent" agents develop a very deep understanding of users in order to provide sophisticated guidance in essential areas of their lives (for instance helping the user throughout the educational process or initiating and supporting the development of a human relationship).

In this context, artificial agents with an understanding of both individuals and social contexts may have important implications for personal identity both at the individual and social level.

**At the individual level**, personal agents may transform users' personal construction of themselves by creating a symbiotic alter ego. In practice, personal agents may help in an individual's self-development by providing feedback, guidance, and relieving the user of repetitive tasks. These agents may also have some negative implications such as the risk of loss of the user's autonomy and excessive dependence ("delegating too much to the agents may mean the agents do not follow the individual's course in life"). They may also encourage the emergence in the society of passive ("why should I bother to make an effort") and individualistic attitudes ("I don't need other people").

The influence of artificial agents on the individual is not fundamentally different in nature from that human agents such as a companions, friends, or instructors can have. Good human agents can, however, be difficult to find even among the relatively favoured social classes (few people can afford a personal tutor, it can take time to develop a trustful relationship, and apparently "friendly" gestures may have other motives).

*By means of techniques such as "collaborative filtering" social agents could help form groups of people with similar profiles and interests and thereby bring people together*

*Artificial agents with an understanding of both individuals and social contexts may have important implications for personal identity both at the individual and social level*

*Although the role of an artificial agent may not differ fundamentally from that of human agents such as friends or instructors, their availability is likely to depend less on socio-economic factors*

## Capturing, managing and protecting personal information

Personal information includes potentially all the information that directly relates to a given individual and which can be exploited to deliver services that take that individual's characteristics into account. The more information a personal agent can extract about a given user, the better able the agent will be to deliver something meeting the user's needs appropriately. Likewise, the more information a social agent has about a group of users, the more effective this agent will be at supporting their social interaction.

A user's information covers a very diverse range of facets such as his or her identity (his/her name, address, and telephone number, email), preferences (e.g. does he/she prefer small or large fonts), skills and qualifications (what domains he/she has experience in, what are his/her university degrees, etc.), interests (what are the areas that motivate him), goals and expectations (does he/she have an "agenda" for career or life development), personality (introverted or extroverted), cognitive style (does he/she like abstraction or does he/she feel more comfortable with concrete cases) or attitude (is he/she a risk taker or risk averse).

Capturing user's information can take a variety of different forms, ranging from the simplest which consists of asking the user to enter information manually, to more advanced techniques by which information is extracted from databases, or to highly sophisticated techniques where the actions of the users are automatically recorded and the information is extracted and categorized using data mining tools.

A user's personal information is very sensitive and needs to be protected. In particular, it is important that the user be guaranteed that highly personal information (such as his or her psychological profile) is only used within the limits of defined boundaries. This kind of protection can be ensured by legal means (typically by prohibiting the recording of certain types of private information). However, excessive regulation at this stage could prevent the development of these new services, and it could be more desirable that protection is achieved both through a combination of technology (to manage the storage and the disclosure of this information in a secure way), and informing users and placing the management of their information under their control (making very clear what systems actually have access to this personal information).

*Personal information covers a wide range of aspects, and the more information an agent has the more effectively it can operate at either the individual or group level. However, at the same time, this raises privacy concerns*

*A combination of technology solutions and providing users with information and control is probably preferable to implementing excessive regulation at this stage*

## Conclusion: intelligent agents represent an opportunity, but are not without risks

Artificial agents represent an important opportunity for the development of radically new services (guidance, support, etc.) which have the potential to transform (or even revolutionize) people's individual and social life. They represent a chance for the less-favoured to mitigate some of the limitations of their environment both at an individual and social level: (1) by providing them the individual assistance (education, advice, motivation) that they could not afford or that would not be available to them otherwise; and, (2) by helping them to acquire the social skills, and in particular how to interact with others and overcoming their lack of social capital.

Intelligent agents also represent an opportunity for society as a whole to benefit from more highly personalized and more effective services, and to develop a richer social life in the many digital spaces that are opening up, and which increasingly occupy a larger part of their life. In particular, they offer users the possibility of developing and managing a much larger and more diverse set of identities and thereby of increasing their degree of personal fulfilment.

However, these agents also pose a number of risks. These include: 1) the risk of increased user

# Identity and Privacy Issues raised by Biomedical Implants

Kevin Warwick, *University of Reading*

**Issue:** Identification implants in humans are now numerous. Investigations are underway linking the human nervous system and computers together. Within a few years trials will have been carried out linking the brain of a normal volunteerto a computer network via an implant.

**Relevance:** Cyborgs, part human part machine, will have abilities well beyond those of humans. The policy and ethical implications of such enhancements of human abilities should be explored.

## Introduction

A cyborg is a person whose abilities have been extended beyond normal human limitations by machine technology[1]. Technology and knowledge puts us in a position where this is not only now possible but where initial investigations, to this end, are already underway. The most important area of concern in this field is the use of chip implants in humans, particularly in terms of their resultant identity and capabilities (See Box 1). Awareness of the possible implications should be raised early on, because in a few years' time cyborg developments may already be well advanced.

We have witnessed many intrusions into the human body. Cochlea implants are now relatively common, as indeed are hip replacements, and heart pacemakers, whilst not being so widespread, continue a trend in which technology is readily accepted as being a necessary intrusion. But each of these represents modifications intended to compensate for deficiencies[3].

The situation lands up on more difficult terrain when, rather than repairing the ineffective parts of a human body, technology is employed to enhance normal functioning. Many examples of such enhancements already exist (although today's examples are primarily "add-ons" rather than implants), particularly in the military domain, such as infrared night sight incorporated into the helmet of a fighter pilot.

*More difficult issues for medical implants are raised when, rather than repairing the ineffective parts of a human body, the technology is employed to enhance normal functioning*

But should such entities present an identity problem? Although the individual's capabilities take on a different form and their abilities are

*The views expressed here are the author's and do not necessarily reflect those of the European Commission.*

influence autonomy. An individual human wearing a night-vision helmet remains an autonomous being. Meanwhile a human whose nervous system is linked to a computer not only puts forward their individuality for serious questioning but also, when the computer is part of a network, allows their autonomy to be seriously compromised.

The main point arising from this is: when an individual's consciousness is based on a nervous system that is part human part machine, questions can be raised as to the human/cyborg character of their moral choices, their identity, and conception of ethics. As a consequence cyborgs may well regard humans with an air of superiority.

We now have machines that many consider exhibit intelligence of their own[4]. In most cases this is distinct from human intelligence and exhibits a number of characteristic properties when compared to human intelligence. Even the most sceptical amongst us agree that "on any issue of computing power, if computers do not have the advantage over human brains already, then they certainly will have before long"[5]. Machines can sense the world far beyond the abilities of humans to the extent that such sensing can be mapped to a series of computations. Using infrared, ultra violet, X-rays and ultrasonics the world can be perceived very differently. Humans also have the problem that they are limited to visualizing the world around them in no more than 3 dimensions. Computers meanwhile are quite capable of dealing with hundreds of dimensions, and realizing relationships involving those dimensions.

Probably the biggest advantage of all for machine intelligence is communication. In comparison with the capabilities of machines, human communication is extremely poor in terms of precision and speed. Humans start with a complex set of electro-chemical signals in their brain and convert them to very slow, mechanical sound, signals in order to speak to someone else. A human recipient then converts the sound signals back to electro-chemical form and tries to arrive at some sort of understanding of what the original signals were all about, with a resultant high error rate partly due to serial transmission - though also with a high degree of tolerance to errors and ability to extract meaning out of messages often full of ambiguities. In comparison, machines can communicate round the world, with very little/no error, with millions of messages being successfully transmitted and received in parallel.

Overall therefore, from a human point of view, a number of distinct advantages can be accrued by becoming a cyborg, as long as human brain advantages such as resilience, tolerance to ambiguity, etc. are preserved. In particular when a human brain is linked, via an implant, to a computer, it opens up the power of the machine to the implanted individual. A human receiving an implant may well then be able to:

- use their computer part for rapid maths
- call on a high speed, internet knowledge base
- have memories they have not had
- sense the world in a plethora of ways
- conceive reality multi-dimensionally
- communicate by thought alone.

All of the above might appear to be valid reasons for an individual human to enhance his abilities through cyborg technologies. But what might the cost be? What might the consequences be? What about the problems associated with actually becoming a cyborg?

Clearly the realization of cyborgs raises enormous questions that affect all aspects of human society and culture. Standing still is not an option. In the extremes, if humans, en masse, opted for a non-cyborg future, could the result be an intelligent machine superculture? Conversely, if humans, en masse, opted for a cyborg future,

*Implanting devices in human beings in order to enhance their capabilities presents enormous questions that affect all aspects of human society and culture* provided the corresponding centres in the cerebral cortex are uniquely identified. Meanwhile sending signals from nervous system to nervous system, which is what is happening now, and ultimately from brain to brain opens up a new form of communication that is far more powerfully immediate than anything that humans possess at present.

Perhaps the key issue though is the competition situations that will emerge. A perhaps less important facet is the competition between technology providers and suppliers as the new market opens up. For society as a whole the key issue may well be competition between those that have implanted technology, and hence exhibit super human abilities, and those who do not. At this stage it is difficult to predict how members of each group will treat those in the other group.

## Conclusions

Picking out important areas for research is not difficult. We need a better understanding of neurology. Not only more knowledge about how the human brain operates but also how to interface directly with it via implants and how such implants will themselves affect the brain's operation. Coupled with this is a deeper understanding of signals measured and the effects of injecting signals. Finally the technology employed for implantation and interfacing, although already developing, needs to be taken forward rapidly in order that the most appropriate connections can be made and the maximum information can be extracted from them.

With an overall brain that is part human, part machine, a cyborg could have extra memory, the ability to conceive in many dimensions and perform high powered mathematical relations, the ability to sense the world in many different ways and to communicate by thought signals alone. Such cyborgs will be far more powerful than humans at tasks that have been reduced to a series of computations. It would also be difficult to imagine that such cyborgs would pay any heed to humans when it came to such tasks/issues. It would be difficult to imagine cyborgs of this ilk wanting to voluntarily give up their powers.

A cyborg's view on life, what is possible and what not, will be very different from that of a human. The values, ethics and identity of a cyborg will relate to its own make up and life, what it feels is important and what not. A cyborg would most likely have a brain, which is not stand-alone but rather, via its machine part, is connected directly to a network. Is it acceptable for cyborgs to give up their individual identity and become mere nodes on a machine network? Is the price to be paid in terms of autonomy, for instance, acceptable to them? Are the implications for competitiveness and identity, among others, acceptable to society? These questions deserve thought as experimentation with cyborg technologies becomes increasingly widespread.

*Privacy issues are immediately apparent even in the case of relatively straightforward identification implants. But even an individual's feelings can, potentially, be modified by electronic means alone if the corresponding parts of the cerebral cortex can be uniquely identified*

# IPTS Publications

- A. Tubke, P. Moncada Paternò-Castello, J. Rojo, F. Bellido, F. Fiore Early Identification and Marketing of Innovative Technologies: A case study of RTD result-valorisation at the European Commission's Joint study of RTD result-valorisation at the European Commission's Joint Research Centre ART 90843 Feb-02
- Andrew Stirling (editor) On Science and Precaution in the Management of Technological Risk. Volume II. Case studies EUR 19056.2 Jan-02
- J. Molas-Gallart, R. Barré, M. Zappacosta, J. Gavigan A Trans-national Analysis of the Result and Implications of industrially-oriented Technology Foresight Studies (France, Spain, Italy) EUR 20138 Dec-01
- K. Ducatel, J.P. Gavigan, P. Moncada Paternó-Castello, A. Tübke Strategic Policy Intelligence: Current Trends, the State of Play and Perspective EUR 20137 Dec-01
- D. Hitchens, F. Farrel, J. Lindblom and U.Triebswetter (editors) The Impact of best available techniques (BAT) on the competitiveness of European industry EUR 20133 Dec-01
- H. Hernández, P. Christidis (editors) Impact of Technological and Structural Change on Employment. Prospective Analysis 2020. Synthesis Report. EUR 20131 Dec-01
- J. Gavigan, F. Scapolo, M. Keenan, I. Miles, F. Farhi, D. Lecoq, M. Capriati, T. Di Bartolomeo A practical guide to regional foresight EUR 20128 Nov-01
- Marcial Echenique y Cia, S.A. LT Consultants Transport and land-use interaction. Part A: Integrated modelling methology EUR 20124 Nov-01
- P. Desruelle, K. Ducatel, J.C. Burgelman, M. Bogdanowicz, Y. Punie, P. Verhoes Techno-economic impact of e-commerce: Future development of value chains EUR 20123 Nov-01
- A. Ekeland, M. Tomlinson, O.B. Ure (co-ordinator) The supply and demand on high technology skills EUR 20122 Nov-01
- P. Jensen Sustainability, Environment and Natural Resources Panel EUR 20119 Nov-01
- E. Gourova Technology, Knowledge and Learning Panel Report EUR 20118 Nov-01

# ABOUT THE IPTS

The Institute for Prospective Technological Studies (IPTS) is one of the seven institutes making up the Joint Research Centre (JRC) of the European Commission. It was established in Seville, Spain, in September 1994.

The mission of the Institute is to provide techno-economic analysis support to European decision-makers, by monitoring and analysing Science & Technology related developments, their cross-sectoral impact, their inter-relationship in the socio-economic context and future policy implications and to present this information in a timely and integrated way.

The IPTS is a unique public advisory body, independent from special national or commercial interests, closely associated with the EU policy-making process. In fact, most of the work undertaken by the IPTS is in response to direct requests from (or takes the form of long-term policy support on behalf of) the European Commission Directorate Generals, or European Parliament Committees. The IPTS also does work for Member States' governmental, academic or industrial organizations, though this represents a minor share of its total activities.

Although particular emphasis is placed on key Science and Technology fields, especially those that have a driving role and even the potential to reshape our society, important efforts are devoted to improving the understanding of the complex interactions between technology, economy and society. Indeed, the impact of technology on society and, conversely, the way technological development is driven by societal changes, are highly relevant themes within the European decision-making context.

The inter-disciplinary prospective approach adopted by the Institute is intended to provide European decision-makers with a deeper understanding of the emerging S/T issues, and it complements the activities undertaken by other Joint Research Centres institutes.

The IPTS collects information about technological developments and their application in Europe and the world, analyses this information and transmits it in an accessible form to European decision-makers. This is implemented in three sectors of activity:

- Technologies for Sustainable Development
- Life Sciences / Information and Communication Technologies
- Technology, Employment, Competitiveness and Society

In order to implement its mission, the Institute develops appropriate contacts, awareness and skills for anticipating and following the agenda of the policy decision-makers. In addition to its own resources, the IPTS makes use of external Advisory Groups and operates a Network of European Institutes working in similar areas. These networking activities enable the IPTS to draw on a large pool of available expertise, while allowing a continuous process of external peer-review of the in-house activities.