September/2002

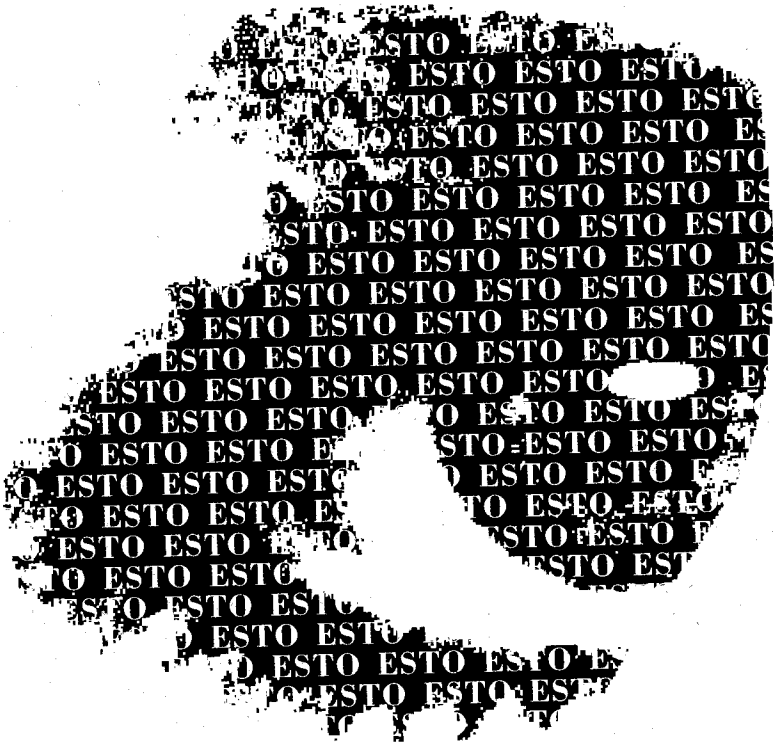
67

ISSN: 1025-9384

5 EURO
EYPΩ

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

CONTENTS

67

SEPTEMBER 2002

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

EDITORIAL BOARD
B. Clements, G. Fahrenkrog, J. Gavigan, M. González, H. Hernández, D. Kyriakou, I. Maghiros (Production Manager), P. Sørup, A. Soria, C. Tahir.

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).

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-

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

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.

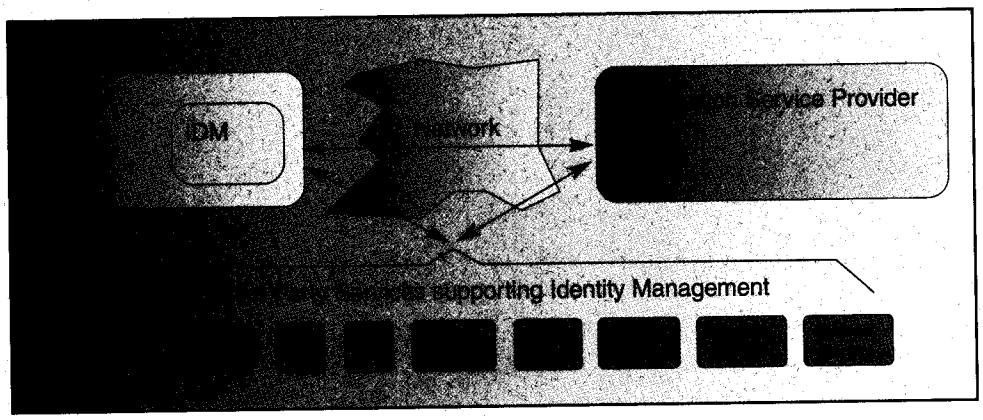
Outlook

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