

Counteracting privacy violations on the Internet

Privacy Online: OECD Guidance on Policy and Practice

26th International Conference on Privacy and Data Protection, Wrocław, 14-16 September 2004

Overview

- A short introduction to the OECD
- Results from the OECD Programme of Work on Privacy Online 1998-2002
- OECD Guidance on Policy and Practice regarding privacy-enhancing technologies
- Conclusions

A short introduction to the OECD

- Membership
 - 30 member countries -- democratic, market economy
 - relations with 70 non-members, private sector, NGOs, civil society
- History
 - Marshall Plan Secretariat, from the Organisation for European Economic Co-operation (OEEC) to OECD
- Objectives
 - Convention of 1961 : growth, job creation, trade, aid for development

Work of the OECD on Information Security and Privacy

- Undertaken in the framework of broader work on Science and Technology and Information and Communication Technology
- Foster trust in electronic commerce and use of information systems and networks
- Privacy, personal data and TBDF
- Security of Information Systems and Networks
- Authentication, cryptography
- Protection of consumers on-line
- analysis of policy options -- inventories, best-practices, "guidelines" (Recommendations)

Trust Policy Framework for Privacy Online

- Security of information systems and networks
- Consumer protection
- Privacy protection
 - 1980 Guidelines
 - 1998 Ministerial Declaration (Ottawa Ministerial Conference)
 - 2002 Report on Privacy Online: OECD Guidance on Policy and Practice (updated version published in 2003)

Why is Privacy Protection a Key Element for Building Trust Online?

- Protecting human rights
- Ensuring free flow of information
- Building trust in the online environment
 - Privacy online is (still) a main consumer concern
 - Protecting privacy is an asset for businesses
 - Networks are global: if businesses want to attract consumers from all around the world, they need to offer sufficient privacy protection tailored to the expectations of their audience

The OECD Privacy Guidelines

- The OECD 1980 Privacy Guidelines represent an international consensus on how best to balance effective privacy protection with the free flow of personal data.
- The Guidelines are technology-neutral, flexible and allow for various means of compliance. They apply in all environments, including on global networks.
- 1998 Ottawa Ministerial Conference: OECD Ministers reaffirmed their commitment to ensure privacy protection on global networks based on the Guidelines, in order to build trust in the online environment.

OECD  OCDE

OECD Privacy Guidelines: The eight principles

1. Collection limitation
2. Data quality
3. Purpose specification
4. Use limitation
5. Security safeguards
6. Openness
7. Individual participation
8. Accountability

OECD  OCDE

OECD “Multi-Door” Approach to Privacy Online

Ministerial Declaration 1998: any global framework for building trust online should be flexible and build bridges between different approaches to privacy

- Integrated approach (regulation and self-regulation)
- Mix of complementary solutions (legal, technical, educational)
- Co-operation among all stakeholders (Governments, Business and Industry, Civil Society)
- Outreach to non-member economies

OECD  OCDE

Privacy Protection Online: OECD Programme of Work 1998-2002

Exchange of information - Analysis

- Inventory of Privacy Instruments and Mechanisms (1999)
- TBDF contracts on global networks (2000)
- Online Alternative Dispute Resolution (2001-2002)
- Compliance and enforcement (2002)

Use of technology

- Privacy Policy Statement Generator (2000)
- Privacy-enhancing-technologies (2001)

OECD  OCDE

2003: Privacy Online – OECD Guidance for Policy and Practice

OECD member countries, businesses and other organisations, as well as individual users and consumers are recommended to give effect to, and disseminate the OECD policy and practical guidance. Non-member economies are also invited to take account of it.



In particular, OECD member countries should take further steps to help ensure privacy protection online at the national and global levels:

OECD  OCDE

Policy recommendations at the national level

OECD Member Countries should take steps to help ensure:

- 1) The adoption of privacy policies
- 2) The online notification of privacy policies to users
- 3) The availability of enforcement and redress mechanisms in cases of non-compliance with privacy principles and policies
- 4) The promotion of user education and awareness about online privacy and the means of protecting privacy
- 5) The use of privacy-enhancing technologies and the development of privacy functions in other technologies, as appropriate

OECD  OCDE

1) *The adoption of privacy policies*

- Encourage organisations with a presence online to:
 - Systematically conduct an extensive review of their privacy practices and to develop a privacy policy that would give effect to the OECD privacy principles.
 - Review data protection laws or self-regulatory schemes, review their own practices against such regulation, and amend practices where necessary to better ensure compliance.
 - Reassess on a regular basis their privacy practices and policy.
 - Use the OECD Privacy Policy Statement Generator.

OECD  OCDE

2) *The online notification of privacy policies to users*

- Encourage organisations with a presence online to:
 - Post their privacy policy online in a prominent place.
 - Conduct regular audits of the accuracy and legal compliance of those policies.

OECD  OCDE

3) *The availability of enforcement and redress mechanisms (1)*

- Member countries should raise organisations' awareness of the benefits of developing effective internal practices and procedures (such as designating CPOs, engaging in voluntary self- or third-party assessment of privacy practices and/or trustmark programmes).
- They should promote effective global solutions with regard to privacy compliance and enforcement by:
 - Fostering the adoption of codes of conduct or trustmark programmes.
 - Fostering the appointment of internal privacy officers in organisations
 - Further providing online resources for handling complaints.
 - Strengthening enforcement against organisations misrepresenting compliance with privacy policies and other privacy promises to individual users.

OECD  OCDE

3) *The availability of enforcement and redress mechanisms (2)*

- Encourage the development and use of fair and effective online alternative dispute resolution (ADR) mechanisms by:
 - Fostering the design and offering of flexible and informal online ADR mechanisms.
 - Striving to reduce national differences in existing legal frameworks that may effect the operability of ADR mechanisms in the cross-border context.
 - Further providing advice to, and raising awareness of individual users on how to file complaints and obtain redress for breaches of their privacy in relation to online interactions.

OECD  OCDE

4) *The promotion of user education and awareness about online privacy*

- Foster effective education and information for organisations and individual users about online privacy protection issues and solutions, including privacy enhancing technologies.
- Further provide online resources for raising awareness about privacy regulations and best practices.
- Raise awareness among individual users for them to better understand the technology and the privacy implications of transactions and interactions on the internet.
- Support academic work to analyse in more detail how to efficiently persuade organisations and individual users to use an effective complementary mix of online privacy protection solutions.

OECD  OCDE

5) *The use of privacy enhancing technologies*

- Actively encourage developers of systems and software applications to incorporate privacy into the design of information technologies.
- Actively encourage organisations to consider at an early stage the privacy implications of their technologies and services.
- Provide incentives, such as appropriate joint action with the private sector, for the further development of a sustainable market for privacy enhancing technologies.
- More generally, educate and raise awareness about technical solutions

OECD  OCDE

Policy Recommendations at the global level

OECD member countries should reaffirm their intention to co-operate to implement the OECD Privacy Guidelines online in the public and private sectors. In particular, member countries should:

- Improve bilateral and multilateral mechanisms for cross-border co-operation between public enforcement agencies.
- Co-ordinate with the private sector and explore how recourse to public/private partnerships could help building trust online in areas where technology and regulation are closely interrelated.
- Promote co-operation with other international organisations as appropriate.
- Explore ways to further online trust across all participants through appropriate outreach, education, co-operation and consultation.

OECD 19 OCDE

Focus on Privacy-enhancing technologies – two years later

- A definition of PETs: "...a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system." (Borking/Raab; JILT 2001/1)
- Examples: cookie manager or –blocker, ad-blocker, anonymous re-mailer, web traffic anonymizer, anti-spyware software ...
- The good news: The idea of PETs has become more widespread (regular workshops, part of research programs e.g. at the national and notably at the EU level)
- Evidence about wide-scale use?

OECD 20 OCDE

Awareness/usage of tools for the protection of data privacy in EU (1)

(source: Special Eurobarometer Data Protection, December 2003)

Q. 34. A lot of personal data are collected when people are on the Internet. Have you heard of tools or technologies limiting the collection of such data? And, if so, have you ever used these tools or technologies?

Country analysis

	No, I have not heard about them	Yes, I have heard about them, but I have never used them	Yes, I have heard about them and I have already used them	Don't know
B	77	15	5	4
DK	68	18	13	2
D.W	69	17	9	5
D.T	74	16	8	4
D.O	77	14	6	3
Gr	81	10	3	7
E	76	16	3	5
F	73	20	4	4
IrI	75	17	3	5
I	74	18	4	4
L	65	24	8	3
NL	59	26	12	3
A	63	23	5	9
P	81	16	2	2
Fin	72	17	8	3
S	58	24	14	4
UK	74	17	6	3
EU15	72	18	6	4

OECD 21 OCDE

Awareness/usage of tools for the protection of data privacy in EU (2)

(source: Special Eurobarometer Data Protection, December 2003)

Q. 35. Why have you never used these tools or technologies?

Country analysis

	Don't know how to install them on my computer	I would not know how to use them	I am not convinced that they work	I am not really concerned about my privacy when I go on the Internet	They are too expensive	Other	DK
B	23	24	21	21	2	13	6
DK	29	25	12	27	6	15	4
D.W	24	34	18	30	5	13	5
D.T	23	34	19	28	6	14	5
D.O	20	32	24	19	13	16	4
Gr	9	35	19	17	4	21	5
E	18	34	17	17	3	13	10
F	18	19	20	19	7	18	13
IrI	22	16	21	13	5	16	15
I	18	34	16	18	5	14	7
L	27	23	24	14	6	14	7
NL	33	31	21	23	6	15	4
A	24	19	12	21	8	23	8
P	10	29	14	19	6	14	11
Fin	19	23	21	31	5	16	8
S	25	27	19	20	6	18	6
UK	21	33	16	14	7	16	8
EU15	21	30	18	20	6	16	8

OECD 22 OCDE

Some conclusions on PETs

- PETs can be an important building block for privacy online within a broader regulatory and self-regulatory framework
- PETs offering control over the transmission of personal data (e.g. anonymous surfing, tools for cookie control) can be especially useful in cross-border situations where the level of privacy at the service provider / in the country of the service provider is unknown or felt to be insufficient
- Governments can influence the development by including PETs concepts in their own services (e-government)
- Further need for raising awareness with users about the existing PETs
- Education of users (use of PET tools AND computer literacy in general) still a priority
- PETs as stand-alone tools may only be part of the solution (i.a. difficulties in turning PET into a business)
- PETs as a concept or mindset can and should be a core methodology for designing information systems and networks (hard- and software)
- PETs should be built-in "off the shelf" into commonly used standard online tools (e.g. browsers, FTP clients) ("privacy by design")

OECD 23 OCDE

Thank you!

Sven Moers

Directorate for Science, Technology and Industry (DSTI), OECD

firstname.lastname@oecd.org

www.oecd.org/sti/cultureofsecurity

www.oecd.org/sti/security-privacy

www.oecd.org/sti/consumer-policy

OECD 24 OCDE