

Unclassified

DSTI/ICCP/REG(2001)6/FINAL



Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

03-Dec-2001

English - Or. English

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY**

**DSTI/ICCP/REG(2001)6/FINAL
Unclassified**

Working Party on Information Security and Privacy

REPORT ON THE OECD FORUM SESSION ON PRIVACY-ENHANCING TECHNOLOGIES (PETs)

Held at the OECD, Paris, 8 October 2001

JT00117775

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

English - Or. English

FOREWORD

On 8 October 2001, the Organisation for Economic Co-operation and Development (OECD) held a Forum session on Privacy-Enhancing Technologies (PETs). This Forum was attended by close to 80 participants from a variety of backgrounds, including representatives of government, the private sector, NGOs and academia.

The objective of the Forum was to demonstrate a number of PETs, so Delegates could experience using them first-hand, and to facilitate discussion on:

- The policy implications of PETs and the future of PETs in the wider context of online privacy protection; and
- The challenges of, and methods for:
 - Educating business about the importance of privacy by design and the use of PETs; and
 - Educating individuals about the benefits and limitations of PETs.

This document reports on the Forum and summarises the presentations and discussions that took place. It is preceded by the Orientation Document which provided Forum participants with background information to assist in their preparation for the meeting. This document also includes two studies by consultants for the OECD: one by Laurent Bernat, Director, Projectweb; and the second by Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London:

- The study by Laurent Bernat includes a synthesis of a survey of PETs currently available on the Web, and a table of the surveyed technologies. This study was provided to participants in advance of the meeting to help them gain a better sense of what types of products are available on the market and what their impact could be on safeguarding users' privacy online (Annex I); and
- The research paper by Perri 6 discusses the question of when, for whom, and under what circumstances, "communication" about PETs might work, in the sense of encouraging businesses to supply such tools, and individuals to use them (Annex II).

The Committee for Information, Computer and Communications Policy approved the declassification of this report at its 40th Session on 11-12 October 2001.

It is hoped that the key themes of this one-day Forum will provide the basis for OECD governments and other stakeholders to identify the benefits and limits of PETs for businesses and individual users, and better envision how the development and use of such tools should be further encouraged at the global level.

Copyright OECD, 2001.

Applications for permission to reproduce or translate all or part of this material should be made to:

Head of Publications Service, OECD, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

**REPORT ON THE OECD FORUM SESSION ON
PRIVACY-ENHANCING TECHNOLOGIES (PETs)**

TABLE OF CONTENTS

FOREWORD	1
MAIN POINTS	4
PRESENTATION OF THE FORUM.....	6
Introduction	6
Overview of privacy-enhancing technologies	7
Further background material	10
Forum Session agenda overview	11
REPORT ON THE FORUM.....	12
Welcome and introduction	12
Session I: Overview of the technology	12
Session II: Educating users/consumers and business	16
NOTES.....	21
ANNEX I: A STUDY OF PRIVACY-ENHANCING TECHNOLOGIES	22
Objective, scope and method.....	22
Figures	24
Summary.....	25
Possible future work	27
ANNEX II: CAN WE BE PERSUADED TO BECOME PET-LOVERS?	40
Introduction	40
The structure of the problem of persuasion and what we need to learn	42
Persuading businesses	43
Persuading consumers	52
Bringing business and consumer interest together	60
Conclusion.....	64

MAIN POINTS

The Forum was successful in providing participants with a more practical level of understanding of Privacy-Enhancing Technologies (PETs), their functionalities, and the extent to which they can help protect privacy. In this respect, the presentation of the survey of 135 Web sites offering PETs gave a clearer picture of what PETs are available today. The Forum also provided an opportunity to generate discussion and establish common understanding on the range of emergent policy issues surrounding the use of these technologies, including those related to education. The main points that emerged from the Forum are highlighted below.

PETs have the potential to help protect privacy online within the framework of either legal regulation or industry-led self-regulation

PETs are technological tools that offer a range of functionalities. They can filter “cookies” and other tracking technologies; allow for “anonymous” Web-browsing and e-mail; provide protection by encrypting data or allow for the advanced, automated management of users’ individual data on their behalf. Most of the PETs available today are designed to be used by consumers, fewer are designed to be used by organisations, and even fewer are designed to be used simultaneously by both individual users and business.

PETs can be employed to determine, for example, if a site was in violation of a particular privacy principle (thereby reinforcing transparency/notice) or to block a site from taking a particular action without the user's consent (thereby reinforcing choice). Therefore, in either a self-regulatory environment or one in which there are laws governing privacy, PETs have the potential to ensure that at least some of the fundamental privacy principles that form the standards of privacy practices in either setting are in place.

PETs have benefits and limits: they are part of a wider package of solutions for privacy protection online

As measured against the OECD Privacy Principles, most of the current PETs designed for individual users provide for collection limitation/choice (45%), collection avoidance (40%), and security (27%). However, none of the PETs available provides total privacy protection in line with the OECD Guidelines: more than half surveyed implement only one principle, and only one tool implements as many as five principles.

PETs designed for businesses can automatically monitor and analyse their information collection, use and potential sharing practices. In this way, PETs can help businesses to secure and maintain compliance with their privacy policy. However, to be most helpful to businesses, PETs should be part of a privacy risk management programme.

PETs are therefore necessarily part of the wider package of privacy protection online that includes regulation and self-regulation and other initiatives such as the development and notification of privacy policies, the use of contractual solutions and also the increasing availability of online redress mechanisms as a further option for recourse.

Increasing transparency and wider usability of PETs may strengthen user and consumer confidence

Current statistics still indicate that users and consumers are uneasy when engaging in e-commerce transactions or other activities online that require the entering of personal data. PETs offer a partial solution to this issue, but individual users must also have strong confidence in the ability of PETs to safeguard their privacy if these technologies are to participate in enhancing trust.

One limit of some PETs is that they do not provide extensive information on the organisation behind the technology or other identifying features. Another limit of some PETs is that they are technical and sometimes not simple enough to be used by average consumers. Therefore, to be more effective and more widely used, and to participate in building trust online, PETs need to be more transparent and to offer wider usability.

Educating business and individual users — the first stepping stone

There is an important need for raising awareness about the existence of PETs and facilitating the education of both business and individual users about their benefits/limits and their complementary role in the framework of privacy protection. A broad spectrum of education strategies will be required to tailor these efforts to different target groups in order to effectively promote their use for a maximum benefit.

For business, enterprises need to be reminded of the importance of managing privacy/security risks and given incentives to balance cost so privacy protection starts with business and the burden does not rest as heavily with the consumer. Business may be encouraged through targeted education strategies to recognise the importance of privacy protection in enhancing client trust and developing mutually profitable relationships, and thereby have the necessary incentives to better provide notice to consumers of business privacy practices, and maintain privacy during online interactions and transactions. Businesses also need to be reminded of the importance of building in privacy technologies when designing new products.

For individual users, there is a clear need for more and better education to further encourage them to take advantage of PETs when exploring the Web, sending and receiving email, or engaging in other online activities. Given the technical nature of these products, a particular challenge is explaining these technologies in simple language given their complexity relative to the general level of understanding in the community. However, users and consumers will only have trust in technologies if they understand how they operate, how they are implemented and their benefits and limits in addressing privacy needs.

PRESENTATION OF THE FORUM

Orientation Document and Agenda Overview for the Working Party on Information Security and Privacy (WPISP) Session on Privacy-Enhancing Technologies

OECD, Paris, 8 October 2001

Introduction

In the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks, issued in Ottawa, the Governments of OECD Member countries delivered a wide-ranging commitment to ensure that the 1980 OECD Privacy Guidelines¹ “are effectively implemented in relation to global networks.” In particular, they focused on five steps. One of them included encouraging the use of privacy-enhancing technologies.

In the three years since the Ottawa Conference and the Ministerial Declaration, the Working Party on Information Security and Privacy (WPISP) has focused on the implementation of other elements of this five-step programme, including work on contractual solutions, alternative dispute resolution (ADR), the launch of the OECD Privacy Policy Statement Generator (to encourage the adoption of privacy policies and their notification to users), and other efforts to educate users, businesses and governments about online privacy. Over the same time period, there have been significant advances in the development and use of privacy-enhancing technologies (or PETs) as a means of promoting online privacy. Many policy makers see great promise in the ability of PETs to help implement privacy principles, such as those contained in the OECD Privacy Guidelines, within the framework of either industry-led self-regulation or legal regulation.

At the February 2001 meeting of the WPISP, Delegates heard presentations on a US government workshop on PETs² from Wendy Lader of the Department of Commerce and on an inventory of PETs prepared for the WPISP by Lauren Hall of the Software and Information Industry Association, who also was serving as a consultant to the OECD Secretariat on PETs.³ The Working Party discussed PETs and decided to address the policy issues associated with these new technologies in greater detail. Delegates agreed that there is a need for raising public awareness about the existence of PETs and facilitating education about their use and agreed that the use of PETs can complement privacy policies by, for example, empowering users to match their privacy preferences with business privacy practices.

Agreement also was reached at the meeting to hold a special Forum session to focus on PETs in which a number of technologies would be demonstrated. Delegates of the OECD Committee on Consumer Policy (CCP) and consumer representatives would also be invited to attend. Forum participants would experience using PETs and discussion would take place on:

- The policy implications of PETs and the future of both PETs and online privacy protection in general.
- The challenges of, and methods for, educating business about the importance of privacy by design and the use of PETs; and
- The challenges of, and methods for, educating individuals about the benefits and limitations of PETs.

The following overview of policy issues related to PETs was intended to provide information and “food for thought” to Delegates prior to the Forum Session. For a more comprehensive discussion of particular PETs themselves and how the technologies function, Forum participants were encouraged to refer to the materials referenced in the section below entitled “Further background material”.

Overview of privacy-enhancing technologies

Various definitions have been written for privacy-enhancing technologies and their aims:

- Lauren Hall, in her inventory, states their purpose as giving “the individual user or technology manager the capability of controlling if, how much or under what circumstances” information is disclosed and/or processed.⁴
- The European Commission’s Article 29 Data Protection Working Party notes that the concept of PETs “refers to a variety of technologies that safeguard personal privacy, notably by minimising or eliminating the collection or further processing of identifiable data.”⁵
- Herbert Burkert from the German Institute for Media Communication says the term “refers to technical and organisational concepts that aim at protecting identity.”⁶
- The Ontario Information and Privacy Commissioner and *Registratiekamer* of the Netherlands focuses on the role of PETs as being an “identity protector” in their joint study.⁷

In other words, PETs are technological tools that assist in safeguarding the privacy of users and consumers. They most often are viewed in the policy context as operating as part of a wider package of privacy initiatives. Given their broad purpose, it is not surprising that PETs, as currently available or envisioned, take on a range of characteristics. Some filter “cookies” and other tracking technologies; some allow for “anonymous” Web-browsing and e-mail; some provide protection by encrypting data; some focus on allowing privacy and security in e-commerce purchases; some allow for the advanced, automated management of users’ individual data on their behalf.

Indeed, the list could be far longer. Accompanying the rapid rise in Internet use and e-commerce sales has been a similar explosion in the privacy and security technologies known as PETs. This “privacy space” of the economy is now a competitive arena, with many companies hoping to attract the interest of users, businesses, and governments. The influx of privacy and security companies comes as surveys continue to demonstrate that users are uneasy about their privacy when venturing online and, especially, when engaging in online purchases where personal information is often revealed.⁸ There are also indications that individuals want more information about the privacy practices of the businesses and organisations with which they transact.⁹

Benefits of PETs

Advocates of the development of PETs come from industry, privacy organisations and many government agencies in OECD countries. In offering their support, these advocates often point to two strong benefits that PETs offer international policy makers: (i) the technologies can be employed to help achieve some of the internationally recognised privacy principles; and (ii) they can be employed in countries that have chosen either a self-regulatory or legal approach to privacy.

Table 1. PETs and privacy principles

Examples of common types of PETs	Examples of some principal policy effects (based on the OECD Privacy Guidelines)
Anonymity/pseudonymity tools	Collection limitation (or avoidance)
Personal data management tools (such as information brokers and infomediaries)	Collection limitation; security
Notice/choice tools (such as the Platform for Privacy Preferences)	Openness/notice; collection limitation/consent and choice
Marketing/advertising control tools (such as cookie and spyware filters and marketing consent management tools)	Collection limitation; choice and/or consent; security
Security tools	Security
E-commerce privacy/security tools	Collection limitation; Security
Access control tools	Notice, security, use limitation, access by data subjects
Children's privacy tools	Collection limitation/consent
Privacy auditing/compliance tools	Accountability

Advocates of PETs note that the technologies can function in either a self-regulatory environment or one in which there are laws governing privacy. In either case, PETs can help to ensure that at least some of the fundamental privacy principles that form the standards of privacy practices in either setting are in place. PETs users could employ them to determine, for example, if a site was in violation of a particular privacy principle (thereby reinforcing transparency/notice) or could block a site from taking a particular action without the consent of the user (thereby reinforcing choice).

Concerns and limitations

But it is clear that not all PETs receive unanimous endorsement by all stakeholders in the international privacy community. Some technologies have been criticised by some privacy advocates as too weak, or even as deceptive tools to erode privacy instead of enhancing it, or as distractions getting in the way of potential regulation of privacy. P3P, very popular in industry and supported by many privacy groups, has come under fire from some privacy advocates. Consumers International, for instance, said in its 2001 Privacy@net study that some technologies, including P3P, “are designed more to facilitate data sharing than to protect users.”¹⁰

Defenders of PETs would object to many of the charges. For example, the Independent Centre for Privacy Protection of Schleswig-Holstein in Germany issued a strong endorsement of P3P, noting its ability to give users “increased control of what happens to their personal data.”¹¹ However, most defenders of PETs (including the Independent Centre for Privacy Protection) agree that they would not today label PETs as the complete solution for online privacy concerns.

A few examples of the limitations of PETs show why: First, many PETs help protect individuals' privacy when online or help provide notice and consent to users, but cannot guarantee the privacy of information once it is given to an organisation or business. One important concern, therefore, stems from the need to ensure that collected information is treated in accordance with the privacy principles (such as the Use Limitation Principle of the OECD Privacy Guidelines). At the same time, on the other side of the debate, the potential for the complete avoidance of data collection through anonymity tools also raises concerns about a lack of accountability in cyberspace and may worry law enforcement authorities.

Debates also continue over the proper “default” settings for PETs. With the assumption that many (if not most) consumers will not alter or customise pre-set product settings, the default setting gains significance, especially in a discussion of privacy. If a user makes no changes to settings on such products as cookie

filters, for example, how many cookies are blocked, what types of cookies are blocked, and what type of information is given to the user about the cookies that are served to his or her computer would all depend on the default position of the filter. Therefore, concerns are raised that some technologies have default settings that are not privacy-protective enough to count as truly enhancing the privacy of their users. (Conversely, some may also argue that user performance in such activities as surfing the Web would be unduly burdened if the default settings were made too privacy protective, such as by blocking all types of cookies.)

In addition, there are practical concerns about PETs. These concerns include whether the technologies are simple enough to be used by average consumers and whether average consumers are willing to purchase, install and operate PETs as client-side tools on their computers. There are also related questions regarding whether a critical mass of PETs users will grow so as to force changes in privacy practices by Web-site operators, or whether PETs users will be the ones forced to sacrifice performance on the Web for privacy protection. On the business side, firms also might well be concerned about the complexity of integrating privacy tools into their operations and/or products.

Role as a tool

Even given these limitations and concerns, the benefits of PETs ensure that the technologies will be part of the policy mixture that addresses online privacy in the future — as recognised in the 1998 Ministerial Declaration. However, it is important to note that PETs are simply tools, to be used by individual users, businesses or governments. Whether they are implemented in ways that are positive or negative, constructive or obstructive, depends to a great extent on the decisions of those who employ them, not on the tools themselves. (As Burkert writes, “We should not forget that PETs . . . essentially remain technical: They *follow* the normative decision.”)¹² At the same time, it is also important to note that there is a multitude of technologies available under the PETs label. Not all PETs may be as good or as privacy-protective as one would want, and not all may be as bad or as privacy-invasive as one might fear. Not all PETs may spark public-policy arguments against their use, and not all may lead to arguments in their favour.

Need for education

Given that PETs are tools, with both significant benefits and limitations for users and businesses, the need for education becomes clear. Sociology Professor Gary Marx makes this case with regard to the privacy implications of information technology in general, noting: “It is . . . important that the technology be demystified and that citizens not attribute to it powers that it doesn’t have. There is a chilling danger in the ‘myth of surveillance’ when the power of information technology is oversold. On the other hand, when technologies are revealed to be less powerful than authorities claim, legitimacy declines. . . . The potentials and limits of technology must be understood.”¹³

In terms of demystifying PETs and promoting their use for a maximum benefit, there are at least three target audiences for education. First, individual users might want to take advantage of these technologies on a personal basis when exploring the Web, sending and receiving e-mail, or engaging in other online activities. Second, businesses might be encouraged to use technologies that could, for example, help maintain privacy during online sales, better provide notice to consumers of their business privacy practices, and/or improve the access control mechanisms surrounding a business’ databases. Third, businesses might be encouraged to build in privacy technologies when designing new products.

As a result, a spectrum of education efforts would be needed to raise awareness of PETs in all target audiences. All would likely need to include attempts to raise awareness and to ensure that there is an

understanding of what privacy solutions PETs can provide, as well as an understanding of their limitations in fully addressing all privacy needs.

According to a recent survey by Harris Interactive for the Privacy Leadership Initiative, few Internet users are currently taking advantage of PETs.¹⁴ Just 15% report having put software on their computer to shield their personal information, while only 10% have used software that allows them to surf online anonymously and 5% have used software designed to allow anonymous purchases. (The numbers are somewhat higher for heavy online users and lower for light users.)

Further background material

Recent workshops and reports

- US Department of Commerce Workshop (September 2000): <http://www.ntia.doc.gov/ntiahome/privacy/>
- EC Joint Research Centre Workshop (May 2000): <http://dsa-isis.jrc.it/Privacy/>
- EU Article 29 Data Protection Working Party Working Document, “Privacy on the Internet: An Integrated EU Approach to On-line Data Protection” (November 2000) includes discussion of PETs: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf

Overview of PETs

- Overview of privacy tools by Lorrie Faith Cranor of AT&T Labs (September 2000): <http://www.research.att.com/~lorrie/pubs/privacy-tools-sept2000.html>
- “The Reinvention of Privacy” by Toby Lester in *The Atlantic Monthly* (March 2001): <http://www.theatlantic.com/issues/2001/03/lester-p1.htm>
- “Networking Health: Prescriptions for the Internet” by the National Research Council (2000) includes analysis of PETs in relation to health issues (pages 167-174, in particular): <http://www.nap.edu/books/0309068436/html/>

P3P (with some mention of other PETs)

- Assorted papers discussing P3P technology: <http://www.w3.org/P3P/>
- Analysis of P3P by the Center for Democracy and Technology and the Ontario Information and Privacy Commissioner (March 2000): <http://www.cdt.org/privacy/pet/p3pprivacy.shtml>
- “Pretty Poor Privacy” report by the Electronic Privacy Information Center and Junkbusters (June 2000): <http://www.epic.org/Reports/pretypoorprivacy.html>

Advocacy group guides to PETs

- Center for Democracy and Technology: <http://www.cdt.org/privacy/pet/>
- Electronic Privacy Information Center: <http://www.epic.org/privacy/tools.html>

Recent international Internet privacy study

Consumers International report on privacy on the Internet, containing an appendix with a discussion of PETs (January 2001): <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf>

Forum Session agenda overview

WELCOME AND INTRODUCTION

Welcome and introductory remarks, *WPISP Chair and Secretariat*

MORNING SESSION: OVERVIEW OF THE TECHNOLOGY

PETs products: overview demonstrations

Overview presentation of PETs available on the Web, *Laurent Bernat, Director, Projetweb; Consultant*

Demonstration of PETs products designed for individual users:

Policy effect of collection limitation/avoidance

Laurent Bernat, Director, Projetweb; Consultant

@nonymouse (@nonymouse.com)— (anonymity/pseudonymity tool)

The Cloak (the-cloak.com) — (anonymity/pseudonymity tool)

Privacy Companion (idcide.com) — (cookie filter)

Netscape 6.1 (AOL-Netscape) — (cookie filter and password manager)

Demonstration of a PETs product designed for both individual users and businesses:

Policy effect of openness/notice, collection limitation/consent, choice

P3P (World Wide Web Consortium) — (server side)

Helena Lindskog, System Manager, Ericsson Infotech

Internet Explorer 6 (Microsoft) — (client side)

Isabelle Valet-Harper, European Standards Manager, Microsoft Europe

Demonstration of a PETs product designed for businesses: Policy effect of accountability

WebCPO (watchfire.com) - (privacy auditing/compliance tool)

Norman McConkey, Director, Watchfire Ltd.

Exploring the technology hands-on

During this agenda item, participants were invited to use those demonstrated PETs designed for individual users. They were invited to split into small groups on computers that were provided by the OECD. Assistance was provided by representatives of the organisations whose technologies would be used, and by the OECD. Questions, as well as discussion among participants, were encouraged.

General discussion, questions and answers

AFTERNOON SESSION: EDUCATING USERS/CONSUMERS AND BUSINESSES

Privacy risk perception and education about PETs

*Perri 6, Director of the Policy Programme of the Institute for Applied Health and Social Policy
King's College London*

Privacy-by-design

Stephanie Perrin, Chief Privacy Officer, Zeroknowledge

Educating consumers about PETs

Naja Felter, Policy Officer, E-Commerce and Trade, Consumers International

General discussion and concluding remarks

Concluding remarks and preview of WPISP policy discussion, *WPISP Chair and Secretariat*

REPORT ON THE FORUM

Welcome and introduction

The Forum Session was opened by **Peter Ford**, Chair of the OECD Working Party on Information Security and Privacy (WPISP). Mr. Ford welcomed the participants to the Forum. He recalled that technology, and in particular PETs, were perceived in the 1998 OECD Ministerial Declaration as an important element of the policy mixture needed to ensure online privacy protection and have been examined thus far by the WPISP in this regard.

Introductory remarks were made by **Anne Carblanc** of the OECD Secretariat. Ms. Carblanc gave a brief overview of each of the presentations to be provided and the running of the Forum. She then broadly described PETs as ‘tools to assist in safeguarding privacy’ and stressed that, in the policy context, they appear to be part of a necessary package of solutions aimed at securing effective online privacy protection for users. She then spoke of the wider objectives of the Forum and the WPISP’s work on PETs generally — that is:

- On the one hand, to identify the benefits and limits of PETs and under what circumstances their development and use should be further supported at the policy level; and
- On the other hand, to examine how to best raise consumer and business awareness of PETs and their role in the broad spectrum of privacy protection, in order to foster the supply and demand of such tools in the interest of privacy protection online.

Session I: Overview of the technology

This Session focussed on allowing participants to gain a better practical-level understanding of PETs as they exist today. Overview demonstrations of selected representative technologies designed for use either by individual users or businesses were given. Participants were then invited to use, in small groups, those technologies designed for individual users, on computers that were provided by the OECD. Assistance was provided both by representatives of the organisations whose technologies were used and the OECD.

PETs products: overview demonstrations

Overview presentation of PETs available on the Web

Laurent Bernat, Director, Projetweb, provided an overview of a *Study of Privacy-Enhancing Technologies* (see Annex I) which he undertook in the capacity of consultant to the OECD. Mr. Bernat explained that the aim of the study was to identify the PETs used on the Internet and to show their impact on privacy protection in light of the *OECD Guidelines for the Protection of Privacy and Transborder Dataflows of Personal Data*.

Mr. Bernat explained that over 130 sites were visited during the study and 83 sites selected for further analysis. He emphasised that the PETs analysed were selected according to their functionality and noted

that the study was not exhaustive — it did not include examination of pure cryptography tools, tools for protecting children, deletion tools, tools designed to protect the PC network or anonymous security tools.

The results of the survey indicated that the PETs available today offer a range of functionalities with a number offering more than one functionality. Most of them are cookie filters (about half); anonymisers occupy 36%; and encryption, ad filters, and mail privacy are just under 20% each. Further, the study revealed that 80% of the PETs surveyed targeted individual users, 20% targeted organisations and 3% targeted both individual users and business.

As measured against the OECD Privacy Principles, the study showed that the PETs available today provide, in most cases, for collection limitation/choice (45%); collection avoidance (40%) and security (27%). Further, of the 83 sites examined, 58 PETs related to only one of the eight principles; 22 to two principles; two to three principles and only one to five principles.

A number of general conclusions and other observations were drawn from these results and summarised by Mr. Bernat as follows:

- From a technical standpoint, none of the tools identified uses a full range of functionalities that would make it possible to provide total privacy protection. Users must therefore combine several tools to optimise and ensure their level of privacy protection.
- 51% of the tools examined in the study must be installed on the user's computer which may be an obstacle to uptake and raise issues of compatibility.
- Some sites provide very little information on the organisation behind the PET product and other identifying features which may constitute a psychological barrier to uptake by users; and
- Many sites do make a serious effort to educate users. However, some of the sites focus more on commercial information rather than on technical educational information.

Mr. Bernat concluded that PETs can be of value in helping users to protect their privacy but are complementary to other tools or instruments. He emphasised that in order for users to have confidence in PETs, they need to understand the technology, the way it is implemented and to know who makes the technology available. He noted that consumer education will therefore be of paramount importance if consumer confidence and ultimately use of these technologies is to increase. Finally, he mentioned that a number of areas for possible future analysis were also identified in the study.

Demonstration of PETs products designed for individual users

Mr. Bernat gave a live demonstration of a number of the technologies designed for individual users. These included two anonymisers — *@nonymouse* and *The Cloak*, and two cookie filters — *The Privacy Companion*, and *Netscape 6.1*. While doing so, he explained their basic functionality to participants.

- *@nonymouse* is an interface that permits users to anonymously navigate the Web, send e-mails, and participate in newsgroups.
- *The Cloak* serves as an interface for anonymous navigation of the Web. Furthermore, thanks to an optional encoding function (https), it offers users connected to the Internet through a

local area network a higher degree of anonymity with respect to the administrator of that network.

- *The Privacy Companion* is a tool which is installed on individual users' desktops to filter cookies. It is effective and user-friendly. The Privacy Companion distinguishes between cookies from the site visited and cookies from third-party sites (tracking network).
- *Netscape Navigator 6.1* allows the user to select his/her default preferences concerning cookie management on a site by site basis. It also makes it possible to filter cookies from third-party sites.

Demonstration of PETs products designed for both individual users and businesses

Helena Lindskog provided a presentation on the Platform for Privacy Preferences (P3P) protocol developed by the World Wide Web Consortium, from the server-side perspective. Ms. Lindskog is a System Manager for Ericsson Infotech, a Lecturer of Karstad University and Ericsson representative in the W3C P3P Initiative Working Group.

Ms. Lindskog first discussed the general concept of 'privacy' and noted that privacy can be enhanced in a number of ways — through anonymity; pseudonymity; unlinkability; unobservability; user consent; or legislation.

Ms. Lindskog then described the P3P protocol. She explained that P3P, at its most basic, is a technology that translates a Website's privacy policy into machine readable format so P3P enabled browsers, and other devices, can read the policy and compare it to the consumer's own privacy preferences. She also briefly presented the steps a service provider must follow in order to implement the P3P protocol. These include: (i) developing a written privacy policy (the P3P Guiding Principles document can be used to assist in this); (ii) deciding which policies apply to which parts of their Website; (iii) selecting a generator; (iv) entering information into the P3P generator; (v) creating a policy reference file and storing it in a specific place; and (vi) using the P3P validator to check if any errors have been made.

In outlining the benefits and drawbacks of the protocol, Ms. Lindskog expressed the view that the protocol does what it is meant to do well — that is, it provides a way for users to consent/not consent to the use of their data by a Website.

Isabelle Valet-Harper, European Standards Manager, Microsoft Europe, provided an overview of the operation of P3P from the client-side perspective through the use of Internet Explorer 6.

Ms. Valet-Harper first broadly described the privacy context and the place of P3P from the user's perspective. She noted that P3P enables users to have their user agents (*e.g.* browsers) act directly on their behalf, or facilitate decision-making regarding their privacy preferences. She noted, however, that P3P is only part of the solution — it helps users to understand privacy policies but other aspects including seal programs and regulations; anonymity tools; encryption tools; laws and codes of practice also play an important role.

Ms. Valet-Harper then spoke in detail about Internet Explorer 6 and its implementation of P3P. She noted that Microsoft's goal for end-users in implementing the technology is to help the user communicate their privacy preferences in an unobtrusive way. She stressed that the focus had been on providing more information about cookies and user choices in relation to cookies, creating smarter automated behaviour and providing the ability to discriminate cookies according to purpose.

Ms. Valet-Harper then provided a demonstration of Internet Explorer 6. She explained that a status icon appears every time a cookie is restricted based on the user's privacy settings — that is when the site being visited uses cookies and the privacy policy of that site does not match the user's settings, cookies are restricted and the user is notified. A user can set his/her individual privacy settings on a 'privacy tab slider' (and elect one of six levels of protection — *i.e.* Accept all cookies; Low; Medium; Medium-high; High; Block all cookies) or he/she can allow the default settings to apply. When the icon appears, the user can also double click the icon to access a detailed privacy report.

Demonstration of a PETs product designed for businesses

Norman McConkey, Director, Watchfire Ltd, provided an overview of the operation of 'WebCPO' a privacy auditing tool for business developed by Watchfire Ltd.

In setting the context, Mr. McConkey noted that because the Internet information and commerce market is global and the Internet's characteristics have accelerated the trend toward increased information collection, use and sharing, organisations must now consider how the laws regulating business and issues arising from privacy breaches around the world will affect them. He further noted that issues relating to privacy on the Web are resulting in widespread market backlash for business such as lost revenue and business opportunities or brand and reputation erosion. All these factors combined emphasise that Website privacy management is critical for businesses which must act to maintain their users' trust if they are to maximise the opportunities afforded by the Internet and have good profitable relationships with users.

Mr. McConkey then discussed the key Web privacy risks for business. He noted that Websites capture a significant amount of sensitive or unnecessary personal information and that privacy leaks can occur through inadequate and un-enforced privacy statements; lack of adequate security protections at point of collecting sensitive personal information; use of cookies and 'invisible' Web bugs for tracking purposes or third party links and integrated third party content.

In order to secure and maintain compliance, Mr. McConkey spoke of the importance that business create and maintain a privacy risk management program as a first step. He then provided a demonstration of his company's software — 'WebCPO', which is a privacy management software for Websites that automatically monitors and analyses all Web properties (Internet, intranet, and extranet) so organisations can understand their information collection, use, and potential sharing practices to help avoid privacy glitches. It is designed for large, multi-user environments and works by analysing a Website and storing the results of this analysis in a central database — users can then query the database to automatically generate comprehensive reports that identify areas where there may be privacy problems. In addition, privacy officials and auditors are automatically notified when changes are made to high-risk areas of the Website (such as unauthorised altering of a privacy statement). Mr. McConkey demonstrated the software live by using it to analyse a purpose built 'broken' Website and showed how the various reports can be generated.

Mr. McConkey concluded by noting that most privacy rules are not intentionally broken but companies need to take compliance with these rules and compliance testing more seriously if consumers are to have confidence in e-commerce.

Exploring the technology hands-on

Participants were then invited to surf the Internet using the technologies designed for individual users on computers provided by the OECD at the meeting venue. OECD staff and presenters were on hand to

provide assistance to participants and further explanation of the functionality of the technologies as they were tested live by participants.

General discussion, questions and answers

During general discussion the following arose:

- Mr. McConkey was asked whether Watchfire Ltd. uses a standard when conducting an audit of a Website’s privacy practices and whether the OECD Privacy Guidelines are used as the basis of this assessment. Mr McConkey noted that data protection issues, when they arise in any jurisdiction, usually fall into four categories and include those related to data collection, data sharing, data spillage and maintaining consistency between a company’s intention (*i.e.* its privacy statement) and its action (*i.e.* what is being done in practice). He explained that the Webco program operates by conducting a search of a corporate Website with a view to isolating whether and where these potential issues exist so that staff are able to make any necessary improvements to ensure compliance with relevant laws/principles/guidelines.
- There was detailed discussion/clarification on the P3P protocol and some confusion among participants as to whether it goes further than cookie management. H. Lindskog confirmed that cookie filtering is one aspect of P3P but that it is much more than this — it is a tool to assist users in having ready access to a Website’s privacy policy and to be able to easily compare it to their own privacy preferences. Ms Valet-Harper indicated that, in the context of Microsoft Internet Explorer 6, users are able to use the technology to distinguish between providing information or blocking cookies that communicate personally identifiable information.
- The issue that there is no way of enforcing the reality of the privacy practices presented by PETs was raised. That is, PETs can represent that they offer certain protections but there is often no way of checking whether the level of protection actually provided matches that which the PET has represented it provides.
- It was mentioned that the P3P technology may be anti-competitive — that is, if a Website/enterprise has a good privacy policy but does not implement P3P, would not its traffic be diverted?
- Finally, the question of whether it would be appropriate to work towards the development of international management standards (which is currently being examined in the European context) was raised.

Session II: Educating users/consumers and business

This session focussed on highlighting through a series of presentations, the challenges of, and methods for educating users/consumers and businesses about PETs. In this session, an academic provided an overview of the nature of privacy risk perception among individuals and how education about PETs fits into this framework. This was followed by two speakers focusing on a more pragmatic level — one on the concept of “privacy-by-design”, and one on the education of users/consumers.

Privacy risk perception and education about PETs

Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, Kings College, London presented his research paper which he undertook in the capacity of consultant to the OECD (see Annex II). Mr. 6 explained that he would concentrate on the inter-relationship between privacy risk perception and education about PETs.

One of the key points Mr. 6 made in his presentation was that when designing effective education for business and consumers, the issue of education needs to be examined as a *persuasion* issue. By this, he meant that the issue of whether or not businesses can be persuaded to invest in PETs — and that consumers can be persuaded to ask for them — is the key to determining when, for whom and under what circumstances ‘communication’ about PETs will be most effective.

For business, Mr. 6 stressed that the challenge is one of persuading them that they should internalise certain costs (to invest in PETs) in a market where they fear their rivals may externalise such costs. For consumers, he noted that the challenge of persuasion is shaped first, by the extent to which different types of consumers care about privacy risks and which risks they care about most; second, how preferences for protection against various kinds of risks are traded off against price increments; and third, how consumers will trade off their privacy preference against the cost of searching out and moving to another supplier.

Further, Mr. 6 asserted that ‘who can be persuaded of what’ needs to be considered bearing in mind differing and particular perceptions of risk. His argument is that not everyone is equally open to persuasion about everything but that classifying and segmenting businesses and consumers can assist understanding of varying levels of ‘openness’ to persuasion on the basis that it is location and institutional context that determine what information one can hear, accept and also what information one will reject.

In his analysis of ‘openness’ Mr. 6 first segmented the populations of businesses and consumers in relevant ways stressing that it is through distinguishing sectors of firms and by grouping consumers according to their situation in social organisation that risk perception can be explained. He separated business for example into the *criminal sector*, the *orderly sector*, the *entrepreneurial sector* and the *sector under the spotlight* and characterised consumers into the groups of *isolate*, *hierarchy*, *individualism* and *enclave*. He then identified which kinds of privacy protections would be expected to be of greatest interest in each segment/group and then discussed the means by which persuasion might be applied most effectively to each of these segments/groups.

Mr. 6 then discussed the dynamics of the relationship between business’ ability and willingness to offer privacy-respecting services and consumers’ ability and willingness to demand those services. He noted that it may be possible for the institutional processes governing businesses and consumers to create a sorting process which leads consumers and businesses with similar characteristics, institutional styles and constraints, and responsiveness to similar concerns to gravitate towards each other. He stressed that this sorting process is never perfect given market dynamics but noted that a reasonable level of sorting between the different segments of business and consumers might be achieved.

In concluding, Mr. 6 highlighted the following for public policy makers endeavouring to persuade business and consumers of the value of PETs: there is scope for persuading business and consumers to be interested in PETs but this scope is circumscribed by the fact that certain kinds of PETs will be more attractive to businesses and consumers in certain situations. By bearing in mind the differing constraints, institutional contexts, basic assumptions and outlooks of businesses and consumers, policy makers may be able to target communications about PETs to specific groups of business and consumers in ways that will make a significant difference.

Privacy-by-design

Stephanie Perrin, the Chief Privacy Officer of Zero-Knowledge Systems Inc. gave a presentation entitled Privacy by Design: Thoughts on progress to date.

Ms. Perrin first provided an overview of the Zero-Knowledge experience since the company was founded in 1997 and then described its key products. She explained that the company's first focus was on developing tools for consumers and its flagship product was *Freedom Premium Services 2.2* — the product enabled consumers to regain total control of their privacy; create their own identity; decide what they wanted to reveal to whom; and to protect themselves from being monitored and profiled. However, recognising that customer demand was for privacy and security tools, Zero-Knowledge recently redesigned and replaced *Freedom Premium Services 2.2* with *Freedom Privacy and Security Tools 3.0*. This newly released product is a software package for online security and online privacy protection which consists of a Personal Firewall plus a flexible suite of applications (including a Form Filler/Password Manager, Cookie Manager, Ad Manager and Keyword Alert) that enables consumers to secure their PC against security threats while protecting their privacy and personal information on the Internet.

Zero-Knowledge's other key product is the Enterprise Privacy Manager (EPM) which is a tool aimed at assisting organisations in achieving secure and private management of customer and corporate data within their organisation. Ms. Perrin explained that the product operates as a tool that enables business to identify, analyse, manage and report on the location and handling of customer information throughout the enterprise. Zero-Knowledge developed the product recognising that organisations are collecting and storing an increasing amount of information but are in a difficult position to manage this information effectively. As an automated tool which assists in tackling this issue, the product is aimed at enabling business to reduce operating and regulatory compliance costs, build customer loyalty and trust, and mitigate the risks associated with information management.

In addition to the EPM, Ms. Perrin explained that Zero-Knowledge provides technical consulting, training and development services to assist companies in a number of areas. These include establishing priorities for a business privacy plan, analysing information-handling practices and in tailoring the EPM system to their unique business-operating environment to ensure its smooth integration into the business.

Finally, Ms. Perrin discussed some of the challenges of communicating privacy by design to both consumers and business. She noted a number of key issues including that: the level of understanding of privacy technologies is still very low; consumers are reluctant to pay for privacy/security protection and are suffering from 'information overload' on new issues; business must be reminded of the importance of putting mechanisms in place to manage privacy/security risks and provided with incentives to invest; law enforcement issues and data retention are still problematic and there has been a chilling in the marketplace; authentication issues are still unsolved; and the newest applications (*e.g.* wireless Internet and geo-positioning) are such that the challenge of building in privacy/security protection is a non-trivial issue and perhaps one not able to be surmounted.

Educating consumers about PETs

Naja Felter, Policy Officer, E-Commerce and Trade, Consumers International (CI), discussed issues related to educating consumers about PETs. Ms. Felter started her presentation by providing background information on Consumers International and an overview of its education initiatives. CI promotes public education primarily through release of its various reports, by educating national members groups and through interactions with the international business community. In seeking to educate consumers

effectively particularly in the area of PETs, Ms. Felter noted that the bar must be set low as the people that most need privacy assistance are likely to have low technical knowledge.

Ms. Felter discussed the findings of CI's Privacy@Net publication which reports on a cross-country survey on privacy in e-commerce. The study investigated Websites' data collection practices. Of the 751 sites investigated, 2/3 of sites were found to collect various kinds of personal information but few had privacy policies that provided information on data rights. Further the study found that, of the sites that did have privacy policies, a number were found to be in breach of these policies.

Ms. Felter noted that privacy and security, access to redress and prevention of fraud are of paramount importance to consumers but that PETs can only help consumers seeking to protect their privacy to a limited extent. The key weaknesses of PETs identified include that they do not have a high degree of usability and consumers are therefore not able to make informed decisions and they only cover a subset of the Fair Information Practices of the Privacy Guidelines. Further, Ms Felter noted that PETs are frequently offered as an alternative to legal protections rather than an extension and that this is unfortunate as they are, at the very best, an incomplete remedy.

Ms. Felter concluded by noting that CI encourages the development of new privacy protection technologies as a complement to the legal framework that regulates the collection of data but believes the burden should not be on the consumer in this area. Further, Ms. Felter noted that business should therefore be encouraged to do more work to ensure that PETs better implement and enforce the OECD Privacy Guidelines and have a much higher degree of usability so they are more useful and effective in safeguarding privacy.

General discussion

During discussion, participants asked a number of particular questions on the content of the presentations:

- Perri 6 was asked to indicate the percentage of consumers that fall into each defined category or group as outlined in his study. He noted that people move from group to group as they move between contexts. For example they may be more 'enclaved' about health data than they are about the identity data stored in a supermarket privilege card. He emphasised that in order to understand what drives risk perception, further study is necessary to look at how people from a community behave when the context changes. He also stressed the need for further empirical/economic data in the area of privacy as there is, at present, no good quantitative data available on a cross-national basis. Mr. 6 finally emphasised the importance of tailoring education and persuasion strategies to the particular situation of the audience being targeted.
- Stephanie Perrin was asked to elaborate on the concept of the 'tagging of data' with corresponding privacy rights/obligations and how this might be achieved. She noted that the issue is one of trying to tag data in the first instance recognising that most large organisations are often not sure where the data they receive has come from and what rights were attached to it/promises made when it was received. The idea is therefore to code all rights to information and to stop it at its aperture so the lawyers can then make a decision as to what is to be done with that information.
- **David Banisar**, on behalf of Consumers International, was asked to provide practical examples of educational actions. He explained that the many consumer organisations which constitute its membership undertake a variety of activities including consumer reports, research on privacy, information campaigns through the media/TV, lawsuits and boycotts. CI

is also hoping to see some large groups doing usability testing and verification tests. Consumers International has also released its 'Five Ways to Improve Privacy Online' publication in five languages. The Council of Europe and Electronic Frontier Foundation (EFF) recommendations on how consumers can protect themselves on the Internet were also noted.

- Stephanie Perrin also commented further on strategies for educating business. Zero-Knowledge's strategies include that it has general information on its Website (*e.g.* why businesses need tools), publishes a newsletter, responds to ad hoc questions on privacy issues and holds annual conferences on Privacy by Design with a view to encouraging business to build in privacy to boost customer loyalty and trust. She noted that educating consumers is important but business must also be encouraged to think about these issues seriously.
- With regard to the issues of privacy in the mobile environment, identified as an area that will raise a new set of issues in the future, H. Lindskog stressed that developments in the wireless industry indicate that users will have their identity in a device and privacy issues in this context will therefore need to be re-evaluated.

Concluding remarks

The Chair closed the Forum by thanking speakers and participants for their contributions. He noted the diverse range of issues that had been discussed during the Forum. He also noted the need for further efforts by governments, business, privacy experts and consumer representatives to notably raise the awareness of users and businesses about PETs, build user confidence in these tools, and influence their development in the interest of greater privacy protection.

NOTES

1. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted on 23 September 1980 as a Recommendation of the OECD Council. Text available on the OECD Website, www.oecd.org.
2. <http://www.ntia.doc.gov/ntiahome/privacy/>
3. See DSTI/ICCP/REG(2001)1/FINAL.
4. Ibid.
5. Article 29 Data Protection Working Party, "Working Document: Privacy on the Internet — An Integrated EU Approach to On-line Data Protection," 21 November 2000.
6. Herbert Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision" in *Technology and Privacy: The New Landscape*, edited by P.E. Agre and M. Rotenberg, MIT Press, 1997. Dr. Burkert is at the Institute for Media Communication of the GMD German National Research Center for Information Technology.
7. Ontario Information and Privacy Commissioner and *Registراتiekamer*, "Privacy-Enhancing Technologies: The Path to Anonymity", August 1995.
8. For example: A March 2000 *Business Week*/Harris survey found that 63% of Internet users who have not purchased anything online were "very" concerned that the company they would buy from would use their personal information to send them unwanted information. A September 2000 Gallup poll found that 53% of Internet users were "very concerned" about the privacy of personal information they gave out online, as well as the privacy of their online activities. The *Economist* magazine noted in October 2000 that the most serious obstacle to e-commerce success is "customers' terror of launching their financial details into cyberspace."
9. See, for instance, the findings of focus groups conducted for the "Consumer Privacy in the Information Age" report issued by the National Consumer Council of the United Kingdom in December 1999.
10. See page 33 and, in general, "Appendix 3: Technologies of Privacy".
11. Other agencies from Member countries have similarly issued statements supporting P3P and other privacy-enhancing technologies.
12. Burkert in Agre and Rotenberg (1997).
13. Gary T. Marx, "Privacy and Technology," <http://web.mit.edu/gtmarx/www/privantt.html>.
14. "A Survey of Consumer Privacy Attitudes and Behaviors," conducted for the Privacy Leadership Initiative by Harris Interactive, released 2 April 2001. In contrast to these low numbers for PETs usage, the survey found that significantly higher numbers of people do take other proactive steps to protect their privacy, including reading privacy policies, refusing to give information they consider too personal or unnecessary, and avoiding visiting specific Web sites with dubious privacy practices.

ANNEX I: A STUDY OF PRIVACY-ENHANCING TECHNOLOGIES*

Objective, scope and method

Objective

The objective of this study is to identify the privacy-enhancing technologies (PETs) used on the Internet and show their impact on privacy protection in the light of the OECD Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data.

Scope of the study

The research focused on tools specific to the Web and, to a lesser extent, e-mail. It is not intended to be exhaustive. Our priority was to concentrate on tools with the following functionalities:

Functionality	Definition
<i>Encryption</i>	Significant but not exclusive use of cryptography.
<i>Anonymity / pseudonymity</i>	Makes users anonymous or conceals their identity by using a pseudonym.
<i>Personal data management</i>	Preference management. Any means that makes it possible to select the information collected.
<i>Cookie filter</i>	Cookie filtering or management.
<i>Ad filters</i>	Filtering or blocking of advertising.
<i>Spyware filters</i>	Detection and deletion of spyware (understood as 1/ transparent GIFs or 2/ client-side ad software).
<i>Marketing consent management</i>	Direct marketing solution respecting privacy.
<i>Mail privacy</i>	E-mail protection (security and/or anonymity of e-mail).
<i>Online payment security</i>	Payment security.
<i>Access control</i>	Centralised password management.
<i>Privacy auditing / compliance</i>	Auditing of the means available and their compliance with current protection principles.
<i>Tutorial</i>	Educational application (educational software).
<i>Complex scheme</i>	Complex technical scheme for protecting privacy (such as Encirq).

and their effects with respect to the privacy guidelines:

- Security.
- Collection limitation / choice.
- Collection avoidance.
- Notice.
- Use limitation.

* This study was prepared by Laurent Bernat, Head, Information and Strategy, Projetweb in his capacity as a consultant for the OECD.

- Access.
- Educational tools / information / awareness.
- Accountability.

Due to constraints of time and resources, the tools providing the following main functionalities could not be examined:

- Pure cryptography tools (such as PGP).
- Tools for protecting children (such as MS Kids passport).
- Deletion tools, whether they permanently delete the traces physically left on the disc in general (true deletion) or delete normally the traces left while surfing the Internet (cookies, temporary cache files, history, *etc.*).
- Tools designed to secure the PC network: personal and professional firewalls, anti-virus, packets sniffers.
- Anonymous access security tools, for example, via a biometric system (such as mytec.com).

Nor were solutions such as “service bundles” proposed by Internet Service Providers (ISP) and hosts taken into account.

Method

Research on the tools targeted was carried out using:

- Major general directories (yahoo.com, about.com).
- Search engines (google.com, alltheweb.com).
- Downloadable software (download.cnet.com).
- Reference sites in the field of privacy protection (epic.org, cdt.org, *etc.*).

Over 130 sites were visited. Some 83 were selected as providing a privacy-enhancing tool on the basis of the criteria selected.

We eliminated from the final list sites that were:

- Clearly obsolete.
- Deemed to have low credibility given their content (*e.g.* an anonymizer that devoted half of its home page to touting the aphrodisiac effects of pheromones¹).
- Presenting products not yet available, even in beta version.
- Unavailable or inaccessible at the time of the test (these sites were visited several times).

It should be pointed out that the fact that a site is functioning does not always mean that the company responsible is still in business.

Each tool was analysed on the basis of:

- The presentation of the product available on the site.
- A short test, if necessary.

The results of this analysis are listed in a breakdown (see attached table) that shows:

- Information about the company: organisation name and URL, type of organisation, founding date, geographic origin, privacy policy on Web Site.
- The name of the product and, if applicable, its version.
- Information about the product: characteristics, principal functionality, policy effect in the light of the OECD Guidelines, principal target audience.

Figures

The figures obtained can be broken down as follows:

Number of sites targeted and selected	83	
Targeted audience		
Individual	69	83%
Organisation	17	20%
Geographic origin		
United States	63	76%
Canada	6	7%
International (such as W3, OECD)	3	4%
?	2	2%
Germany	2	2%
Russia	2	2%
France	1	1%
Gibraltar	1	1%
Sweden	1	1%
Thailand	1	1%
United Kingdom	1	1%

As the research was conducted using keywords in English, it is possible that some tools may not have been identified if the sites presenting them were drafted in another language. This may explain the fact that there were few tools on sites other than North American ones.

Privacy policy on the Web Site		
Yes	63	75%
No	20	25%
Type of application		
Web based	24	29%
Install.	42	51%
Web based / install.	4	5%
Install (java).	2	2%
Install (ActiveX).	1	1%
Other	10	12%
Pay or Free?		
Pay	30	36%
Free	38	46%
Both	11	13%
Not clear	4	5%
Registration required	9	11%

Subscription required	14	17%
Principal functionality		
Encryption	16	19%
Anonymity / pseudonymity	30	36%
Personal data management	10	12%
Cookie filter	39	47%
Ad filters	15	18%
Spyware filters	15	18%
Marketing consent management	2	2%
Mail privacy	15	18%
Online payment security	4	5%
Access control	5	6%
Privacy auditing / compliance	6	7%
Tutorial	2	2%
Complex scheme	7	8%
Policy effect		
Security	22	27%
Collection limitation / choice	37	45%
Collection avoidance	33	40%
Notice	11	13%
Use limitation	2	2%
Access	2	2%
Educational tools / information / awareness	2	2%
Accountability	4	5%

Summary

An examination of the characteristics of these tools and an assessment of their limitations confirms that they can be of value in helping users to protect their privacy, but also that they are necessarily complementary to other tools (educational, contractual, regulatory, *etc.*).

Benefits and limitations

From a technical standpoint, none of the tools identified uses a full range of functionalities that would make it possible to provide total privacy protection in line with the OECD Guidelines.

If we count the number of tools that have an impact on the OECD Guidelines, we see that:

- Only one tool concerns five of the eight principles².
- Two tools concern three principles.³
- 22 tools concern two principles.
- 58 concern only one principle.

Consequently, no tool identified in this study provides a complete solution for privacy protection. Users who wish to protect themselves most effectively should therefore combine several tools to optimise their level of protection.

Permission marketing and privacy: the birth of a new market?

The tools and solutions discovered in this study constitute an emerging market, and users' demand for privacy protection is being met by a supply that is divided into a number of segments. Some companies are proposing original solutions involving technological intermediation (similar to the concept of "infomediary" developed by John Hagel and Marc Singer⁴) aimed at enabling companies to use personal data for marketing purposes with users' consent (permission based marketing) while guaranteeing respect for their privacy. These companies appear to have been established quite recently and are currently looking for economic and financial partners.⁵

Technical barriers to wider use

51% of the tools examined in this study must be installed on the user's computer. This can sometimes be an obstacle to their wider use for the following reasons:

- Users may view this process as being potentially dangerous and refuse to install the tool.
- It may go against company policy, since companies often prohibit employees from installing non-standardised applications on their computers; this would place employees in an ambiguous situation vis-à-vis their employer and make them take conflicting risks in order to protect their privacy.

Furthermore, for a product to be widely used, it must be compatible with all the user systems available, and, when used as a browser plug-in, it must be available for a number of browser versions. In reality, these products are rarely this flexible, as their publishers concentrate on making them compatible with one or two versions of the user systems or browsers on the market.

Psychological barriers: the importance of trust

Some sites provide very little information on the organisation behind them, their country of origin, their nature (commercial company, association, natural person, *etc.*), the identity of their founders or even their exact address and telephone number. Often, an e-mail address is the only connection between the user and the publisher of the site.

Some free sites provide no information that would enable users to identify their origin, even by querying the Whois database in order to identify the owner of the site's name.⁶ As for pay products, which require remote payment in order to use the product, they do not always provide the information necessary.

Internet users will only use PETs type tools if they can trust:

- The technology used by the tool. This means that users must understand this technology and what it can provide.
- The tool itself: is it reliable, without defects or bugs that, instead of protecting users, might make them more vulnerable?
- The organisations or individuals who developed the tool: are they really pursuing the goals that they say they are?

The software developed by the Open Source community provides a high level of transparency. A number of Open Source projects being developed are specifically aimed at privacy protection.

Educating users

As the preceding summary shows, educating users is an indispensable component of the policy mixture that addresses online privacy. In this regard, many of the sites visited make a serious effort to educate users as a necessary preliminary for persuading them to use their product.

In this regard, three different approaches can be distinguished in the sites visited:

- Sites presenting technologies that are being developed and that are therefore intended mainly for advanced users, whether they are power-users or developers.⁷ In this case, the information is highly detailed and technical, and probably too complex for final users.
- Sites that combine their commercial documentation or the presentation of their aims with high-quality educational information⁸ and links to other reference sites.
- Sites that primarily describe the advantages and benefits of the tool without really informing users of how the benefit provided (such as anonymity) is related to the technical functioning of the product.

Possible future work***Optimising classification of technical functionalities***

A more complete classification of the functionalities and techniques used, together with accurate definitions, would make it possible to describe better how each technology is linked to its policy effect.

For example:

- Regarding cookies, a distinction could be made between display, blocking, filtering, editing, deleting and recognising cookies from other sites. Some tools may limit collection via user choice (collection limitation / choice) or systematically prevent collection (collection avoidance) depending on the functionalities used.
- For anonymity tools using a non-transparent proxy, a distinction might be made between tools that:
 - Use their own proxy.
 - Select, test and use other proxies, thereby considerably increasing the degree of anonymity of the user.
 - Authorise HTTPS to scramble the traces left on the local network.
 - Filter certain information (cookies, last page visited, advertising, javascript, images, *etc.*).

Further investigation of these questions would also make it possible to take certain technical subtleties into account. For example, a persistent cookie is a risk for users of the site that sets the cookie, but also for third parties that have access to these users' hard disc. This means that cookie management tools might have a "security" policy effect, as understood in the OECD Guidelines.

Specific studies on certain types of tools

Specific studies might be carried out on the technologies that have not been analysed, such as:

- Pure cryptography tools.
- Tools related to e-mail use.
- Personal security tools.
- Tools designed more specifically for children.
- Tools using other protocols besides e-mail or the Web, such as newsgroups, chat rooms (ICQ, IRC, AOL's buddy list, *etc.*), telnet or file transfer (FTP) that have not been specifically addressed in this study, even though they are now widely used.

Special attention should be focused on:

- Tools being developed in the free software community: when the keyword "Privacy" was entered in the search engine of the main site that lists these projects,⁹ it showed some 25 projects under way.
- Projects that use distributed network or peer-to-peer (P2P) technologies, especially the Freenet project aimed specifically at ensuring the anonymity of its users, whether they are publishing or using information.
- Tools and technologies intended to ensure the security of a system or access to a system without divulging the identity of users (such as, mytec.com, mentioned above).
- Tools and solutions oriented towards permission-based marketing, which respect the privacy of users.

Usability of tools and educational aspects

An analysis of the usability of tools might provide an interesting perspective. This would mainly involve evaluating the ability of final users to grasp fully the purpose of each tool, install it effectively and use it continuously on a daily basis.

Although few tools are primarily aimed at educating users and enabling them to take responsibility for protecting their own privacy, most of them do help keep users better informed and some give this aspect great importance. It might be interesting to identify the tools that have specific functionalities for this purpose and to analyse the means that they use.

Other possibilities

More in-depth research on the tools available, *i.e.* aimed at compiling an exhaustive list, might be carried out, in particular by using search terms in other languages besides English.

NOTES ON ANNEX I

1. <http://www.aixs.net>
2. Auditing/compliance tool for businesses (TrustFilter, a product of PrivacyRights).
3. Freedom Internet Privacy Suite, a product of Zero Knowledge, for Internet users, and IBM's Tivoli Secure Way Manager, for organisations.
4. "Net Worth", Harvard Business School, 1999.
5. For example, the solutions available from Lumeria, Encirq and Persona.
6. For example: www.the-cloak.com, a Web interface that make it possible to anonymise Web surfing via a proxy. No information on the origin of the service or the identity of the service providers is available on the site. On the basis of the information on the Whois database, it is not possible to identify clearly its country of origin.
7. For example, the site of the Freenet project (<http://freenet.sourceforge.net>) or of IBM's P3P policy editor (<http://www.alphaworks.ibm.com/tech/p3peditor>).
8. For example, Anonymizer's site presents clear information on how the product works and, by extension, on the principle of proxy anonymizers (<http://www.anonymizer.net>).
9. <http://www.sourceforge.net>

Table 1. Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
@nonymouse @nonymouse.com	association	1997 (copyright)	Yes	Germany	AnonWWW AnonEmail AnonNews	Free. Web based.	Anonymity / pseudonymity. Mail privacy.	Collection avoidance.	individual.
AbsoluteFuture, Inc. www.safemessage.com	software company	1998	Yes	United States	SafeMessage v. 2.0	Pay. Subscription required. Install.	Encryption. Mail privacy.	Security. Collection avoidance.	organisation.
adScience, Ltd. www.adscience.co.uk	software company	1997 ?	Yes	United Kingdom	Filtergate v. 4.03	Pay. Install.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
Agenetics www.superyou.net	Internet company	?	Yes	United States (domain name)	SuperYou Messaging	Free. Registration required. Web based. Beta version.	Encryption. Mail privacy.	Security.	individual.
American Express www.americanexpress.com	credit card provider	1850 (Private Payments : 2000)	Yes	United States	Private Payments	Free. Registration required. Install. Free for cardholders.	Online payment security.	Security. Collection limitation / choice.	individual.
AnalogX www.analogx.com	software company ?	1998 ?	No	United States	CookieWall v. 1.01	Free. Install. Adds on to browser.	Cookie filter.	Collection limitation / choice.	individual.
Anonymizer www.anonymizer.com	privacy/security company	1996	Yes	United States	Anonymous Surfing, Secure Tunneling	Pay. Subscription required. Web based / install. Very basic is free.	Anonymity / pseudonymity. Cookie filter. Ad filters. Spyware filters.	Collection avoidance.	individual.
AOL/Netscape www.netscape.com	ISP/software company	?	Yes	United States	Netscape Cookie Manager, Password manager v. 6.1	Free. Included in browser.	Cookie filter. Access control.	Security. Collection limitation / choice.	individual.
Ascentive www.ascentive.com	software company	1998 (copyright)	Yes	United States	ActivePrivacy v. ?	Pay. Install. Free for a limited time.	Cookie filter.	Collection limitation / choice.	individual.
AT&T www.research.att.com/projects/crowds	Telecommunica-tions company	AT&T founded in 1875	Yes	United States	Crowds	Free. Registration required. Install. Only for non commercial use in the United States.	Anonymity / pseudonymity.	Collection avoidance.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
AT&T www.research.att.com/projects/p3p/propgen	software company	AT&T founded in 1875	Yes	United States	P3P proposal generator	Free. Web based.	Personal data management.	Notice.	individual.
Barefoot Productions www.barefootinc.com	software company	1994 (incorporated 1997)	No	United States	Zdnet's CookieMaster v. 2.0	Free. Install. Product outdated (only for IE 3.0). Distributed by ZiffDavis, the links to zdnet are broken.	Cookie filter.	Collection limitation / choice.	individual.
Basta Computing www.basta.com	software company	1996	Yes	United States	Buzof v. 1.6	Pay. Install.	Cookie filter. Ad filters.	Collection limitation / choice.	individual.
Camtech 2000, Ltd. www.camtech2000.net	software company ?	?	No	United States (domain name)	CT Cookie Spy v. 2.0	Free. Install.	Cookie filter.	Collection limitation / choice.	individual.
Checkflow www.checkflow.net	software company	?	Yes	France	FlowProtector v. 2.0	Free / pay. Install. Pay for advanced version.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
Direct Marketing Association www.the-dma.org/library/privacy	trade association	1917	Yes	United States	Privacy Policy Generator	Free. Web based.	Personal data management.	Notice.	organisation.
Disappearing Inc. / Omniva www.disappearing.com www.omniva.com	software company	1999	Yes	United States	Omniva Policy Manager v. ?	Pay. Install.	Encryption. Online payment security.	Security.	organisation.
Distinctly.com, Inc. www.silentsurf.com	Internet technologies company	1997 (domain name)	Yes	United States	SilentSurf	Free. Web based.	Anonymity / pseudonymity.	Collection avoidance.	individual.
Ditto Technologies www.dittotech.com	software company	2000 (copyright on the site)	No	United States	Cookie Eater	Free. Install.	Cookie filter.	Collection limitation / choice.	individual.
Ditto Technologies www.dittotech.com	software company	2000 (copyright on the site)	No	United States	MiLk v. 2.0	Pay. Install.	Cookie filter.	Collection limitation / choice.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
Dr. Jon's Software download.at/drjsoftware	individual developer(?)		No	United States	MagicCookie Monster v. 1.0 fc 1a	Free. Registration required. Install. Email registration.	Cookie filter.	Collection limitation / choice.	individual.
Encirq www.encirq.com	privacy / security / marketing services company	1998	Yes	United States	Illuminated Statement	Pay. Business based tool.	Anonymity / pseudonymity. Complex scheme.	Collection avoidance.	organisation.
Eric Murray Consulting www.lne.com/ericm	privacy / security consultant	?	No	United States	Cookie Jar v. 2.01	Free. Install.	Cookie filter.	Collection limitation / choice.	individual.
Free Network Project freenet.sourceforge.net	non profit corporation	1999	No	United States	Freenet v. 0.3.9.2	Free. Install. Beta. version Open source project. The corporation was created only to get donations.	Encryption. Anonymity / pseudonymity. Complex scheme.	Security. Collection avoidance.	individual.
George Mason Society freedom.gmsociety.org	advocacy group	?	No	United States	Freedom remailer	Free. Web based.	Anonymity / pseudonymity. Mail privacy.	Collection avoidance.	individual.
Global Internet Liberty Campaign www.gilc.org/speech/anonymous	advocacy group	?	No	International	W3-Anonymous Remailer	Free. Web based.	Anonymity / pseudonymity.	Collection avoidance.	individual.
Guidescope, Inc. www.guidescope.com/home	Internet technologies company	2000	Yes	United States	Guidescope v. 0.994	Free / pay. Install. Free for personal / pay for business.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
Hidden surf www.hiddensurf.com	Internet privacy company ?	?	Yes	United States (domain name)	Hiddensurf	Pay. Subscription required. Web based.	Anonymity / pseudonymity. Cookie filter.	Collection avoidance.	individual.
Hilgraeve www.hypersend.com	privacy software company	1980	Yes	United States	HyperSend	Pay. Registration required. Subscription required. Web based / install.	Encryption. Mail privacy.	Security. Collection avoidance.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
Hush Communications www.hushmail.com	privacy/security company	1998	Yes	United States	HushMail v. V2	Free / pay. Web based. Free + yearly fee for advanced service.	Encryption. Anonymity / pseudonymity. Mail privacy.	Security.	individual.
IBM www.ibm.com	information technology company	1914	Yes	United States	Tivoli SecureWay Privacy Manager	Pay. Install. Business based tool.	Complex scheme.	Security. Use limitation. Access.	organisation.
IBM www.ibm.com www.alphaworks.ibm.com/tech/p3peditor	information technology company	1914	Yes	United States	P3P Policy Editor v. beta 1.7	Free. Install. Beta version.	Personal data management.	Notice.	individual.
Idcide www.idcide.com	privacy/security company	1999	Yes	United States (Israel)	Privacy Companion v. 1.0.3	Free. Install. Browser add-on	Cookie filter. Spyware filters.	Collection limitation / choice.	individual.
Idcide www.idcide.com	privacy/security company	1999	Yes	United States (Israel)	PrivacyWall (Site Analyzer, Site Monitor)	Pay. Install.	Privacy auditing / compliance.	Accountability.	organisation.
IDzap, LLC www.idzap.com	privacy/security company	?	Yes	United States	- Idsecure - free anonymous browsing	Free / pay. Registration required. Subscription required. Web based. Subscription for advanced service (idsecure). Free for basic (free anonymous browsing). Email registration for both.	Anonymity / pseudonymity. Cookie filter.	Collection avoidance.	individual.
Incogno Corporation www.incogno.com	software company	1999	Yes	United States	SafeZone	Business-based tool	Encryption. Anonymity / pseudonymity. Online payment security. Complex scheme.	Security. Collection avoidance.	organisation.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
iNetPrivacy www.inetprivacy.com	privacy software company	1997 (copyright)	No	Russia / Canada (domain name)	Anonymity 4 Proxy (A4Proxy) v. 2.52	Pay. Install.	Anonymity / pseudonymity. Cookie filter.	Collection limitation / choice. Collection avoidance.	individual.
Information and Privacy Commissioner / Ontario www.ipc.on.ca/english/resources/resources.htm	privacy Commissioner	1990	No	Canada (Ontario)	Privacy Diagnostic Tool (PDT)	Free. Install. MS Access file.	Privacy auditing / compliance. Tutorial.	Educational tools / information / awareness.	organisation.
Intelligent Software Modeling Inc. www.surferprotectionprogram.com	Internet privacy company	1997	No	United States	Surfer Protection Program	Pay. Install.	Cookie filter.	Collection avoidance.	individual.
Intelytics www.intelytics.com	privacy software company	?	Yes	United States	Message sentinel	Pay. Install.	Spyware filters. Mail privacy.	Collection avoidance.	individual.
Intelytics www.intelytics.com	privacy software company	?	Yes	United States	Personal Sentinel v. 1.5.2	Free. Registration required. Install.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
Intelytics www.intelytics.com	privacy software company	?	Yes	United States	Site sentinel	Pay. Install.	Privacy auditing / compliance.	Accountability.	organisation.
Intermute www.intermute.com www.adsubtract.com	software company	?	Yes	United States	AdSubtract	Free / pay. Registration required. Install. Free for personal use / pay for more advanced versions.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
Invisible hand software www.privacybot.com	software company	1991	Yes	United States	PrivacyBot	Pay. Subscription required. Web based.	Privacy auditing / compliance.	Notice. Accountability.	organisation.
iPrivacy www.iprivacy.com	privacy/security company	1999	Yes	United States	Identity Manager	Free. Consumer access tool through credit card companies.	Encryption. Anonymity / pseudonymity. Online payment security. Complex scheme.	Security. Collection avoidance.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
ISL Internet Sicherheitsloesungen GmbH www.rewebber.com	privacy/security company	?	Yes	Germany	Rewebber	Pay. Subscription required. Web based.	Encryption. Anonymity / pseudonymity.	Collection avoidance.	individual.
Junkbusters Corporation internet.junkbuster.com	privacy/security company	1996	Yes	United States	Internet Junkbuster Proxy v. 2.0.2	Free. Install. License : GPL.	Cookie filter. Ad filters.	Collection limitation / choice.	individual.
KeepItSecret www.keepitsecret.com	privacy/security company	?	No	United States (domain name)	KeepItSecret (?)	Free / pay. Web based. Free with registration / daily mailing, pay accounts without mailing.	Anonymity / pseudonymity. Cookie filter.	Collection avoidance.	individual.
Kookaburra Software www.kburra.com	software company	1996	Yes	United States	Cookie Pal v. 1.6	Pay. Install.	Cookie filter.	Collection limitation / choice.	individual.
Lavasoft www.lavasoftusa.com	software company	?	No	Sweden ? United States ?	Ad-Aware, Ad-Aware Plus v. 5.5	Free / pay. Install. Free for basic version, pay for advanced versions.	Spyware filters.	Collection limitation / choice.	individual.
Lumeria, Inc. www.lumeria.com	privacy/security/ marketing services company	1998	Yes	United States	Sunshine technology, including SuperProfile	Beta version business-based tool.	Personal data management. Cookie filter. Ad filters. Marketing consent management. Complex scheme.	Collection limitation / choice.	individual. organisation.
MailEncrypt mailencrypt.com	privacy internet company	1998	Yes	United States	MailEncrypt	Pay. Subscription required. Web based.	Encryption. Mail privacy.	Security.	individual.
Mailsafe www.mailsafe.org	privacy internet company	1998	Yes	Gibraltar	Mailsafe	Pay. Subscription required. Web based.	Encryption. Mail privacy.	Security.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
MetaURL Corporation www.idmask.com	privacy/security company (?)	?	Yes	Canada	ID Mask	Free / pay. Subscription required. Install (java). Free gets limited bandwidth. Subscription gets unlimited. Source code may become publicly available.	Anonymity / pseudonymity. Cookie filter.	Collection limitation / choice. Collection avoidance.	individual.
Microsoft www.microsoft.com	software company	1975	Yes	United States	Internet Explorer 6 (with some P3P elements and cookie filtering) v. 6_PP_Refresh	Free. Beta. version Free download or part of Windows XP.	Personal data management. Cookie filter.	Collection limitation / choice. Notice.	individual.
MishkinSoft www.multiproxy.org	software company	?	No	Russia	MultiProxy v. 1.2	Free. Install. Free for personal use.	Anonymity / pseudonymity.	Collection avoidance.	individual.
Naviscope Software www.naviscope.com	software company	?	No	United States (domain name)	Naviscope	Free. Install. Could become pay in future.	Cookie filter. Ad filters.	Collection limitation / choice.	individual.
NetHush www.nethush.com	?	2001	Yes	United States (domain name)	NetHush	Free. Web based. Financed with ads.	Anonymity / pseudonymity. Cookie filter. Ad filters.	Collection avoidance.	individual.
Orangatango www.orangatango.com	Internet privacy company	2000 (copyright)	Yes	United States	Virtual Browser v. 1.0	Free / pay. Subscription required. Web based. Free for one week trial.	Encryption. Anonymity / pseudonymity. Ad filters.	Security. Collection avoidance.	individual.
Organisation for Economic Co-operation and Development cs3-hq.oecd.org/scripts/pwv3/pwhome.htm	international organisation	1961	Yes	Headquarters in France	OECD Privacy Policy Statement Generator	Free. Web based.	Personal data management. Tutorial.	Notice. Educational tools / information / awareness.	organisation.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
Packetderm, LLC webmail.cotse.com/webmail	privacy/security company	2000	Yes	United States	Cotse Webmail	Pay. Subscription required. Web based. Free web mail closed. Only pay remains	Encryption. Anonymity / pseudonymity. Mail privacy.	Security. Collection avoidance.	individual.
PC Magazine www.zdnet.com/pcmag	media company	?	Yes	United States	CookieCop, CookieCop Plus v. 1.2	Free. Install. Source code included.	Cookie filter.	Collection limitation / choice.	individual.
Persona www.persona.com	privacy/security/marketing services company	1998	Yes	United States	p-CRM platform	Pay. Business based tool.	Personal data management. Marketing consent management.	Collection limitation / choice.	individual. organisation.
Ponoi Corporation www.ponoi.com	privacy/security company	2000 (copyright)	Yes	United States	Ponoi	Install (java). No information about the business model. Seems free.	Encryption. Anonymity / pseudonymity. Access control.	Security. Collection avoidance.	individual.
Potato Software www.skuz.net/potatoware/jbn/about.html	software company ?	?	No	?	Jack B. Nymble v. 2	Free. Install.	Encryption. Anonymity / pseudonymity. Mail privacy.	Security. Collection avoidance.	individual.
Privacy Foundation www.bugnosis.org	advocacy group	?	Yes	United States	Bugnosis	Free. Install (activeX).	Spyware filters.	Collection limitation / choice.	individual.
Privacy Software Corporation www.nsclean.com	privacy/security company	1996	Yes	United States	IEClean, NSClean v. 5.5	Pay. Install.	Cookie filter. Mail privacy.	Collection limitation / choice.	individual.
PrivacyRight www.privacyright.com	privacy/security company	?	Yes	United States	TrustFilter (with special versions for financial services, health care and e-business)	Pay. Business based tool.	Access control. Privacy auditing / compliance. Complex scheme.	Security. Collection limitation / choice. Notice. Use limitation. Access.	organisation.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
PrivacyX.com Solutions www.privacyx.com	privacy/security company	1998	Yes	Canada	PrivacyX, PremiumX	Free / pay. Web based. Web based service is free but with ads (privacyX), more advanced is pay without ads (PremiumX). User must install a certificate and may use their usual mail program.	Anonymity / pseudonymity. Access control.	Security. Collection avoidance.	individual.
Rendering Better Avenues Software www.rbaworld.com	software company	1997 (copyright)	No	United States (domain name)	Cookie Cruncher v. 2.11	Free. Install.	Cookie filter.	Collection limitation / choice.	individual.
SafeWeb www.safeweb.com	privacy/security company	2000	Yes	United States	SafeWeb Triangle boy	Free. Web based / install. Web based for SafeWeb, install for Triangle boy.	Anonymity / pseudonymity. Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice. Collection avoidance.	individual.
SendFakeMail www.sendfakemail.com	privacy/security company	?	No	Thailand	SendFakeMail	Pay. Subscription required. Web based.	Anonymity / pseudonymity. Mail privacy.	Security. Collection avoidance.	individual.
SiegeSoft www.siegesoft.com	privacy software company	1998	Yes	Canada	Siege Surfer	Pay. Subscription required. Web based.	Anonymity / pseudonymity. Cookie filter.	Collection avoidance.	individual.
Spyblocker Software www.morelerbe.com/spyblocker	software company	?	Yes	United States	SpyBlocker v. 4.2	Free. Install.	Cookie filter. Ad filters. Spyware filters.	Collection limitation / choice.	individual.
SpyChecker.com www.spychecker.com	advocacy group ?	?	Yes	United States	SpyChecker v. 1.1	Free. Web based / install.	Spyware filters.	Notice.	individual.
The Cloak www.the-cloak.com	?	?	Yes	?	The Cloak	Free. Web based.	Anonymity / pseudonymity. Cookie filter.	Collection avoidance.	individual.

Table 1 (cont'd.). Table of surveyed technologies

Organisation name and URL	Type of organisation	Founding date of organisation	Privacy pol. on Web site?	Geographic origin	Name of main PETs product(s) and version	Product characteristics	Principal functionality	Policy effect	Principal targeted audience
The Limit Software www.thelimitsoft.com	software company	1994	Yes	United States	Cookie Crusher v. 2.6	Pay. Install.	Cookie filter.	Collection limitation / choice.	individual.
Watchfire www.watchfire.com	Internet technologies company	1996	Yes	Canada	WebCPO	Pay. Business based tool.	Privacy auditing / compliance.	Accountability.	organisation.
World Wide Web Consortium www.w3.org	industry consortium	1994	Yes	International	Platform for Privacy Preferences (P3P) v. 1.0	To be incorporated in browsers and on organisation web sites.	Personal data management.	Collection limitation / choice. Notice.	individual. organisation.
YOUPowered www.youpowered.com	privacy/security/marketing services company ??	?	Yes	United States	Orby v. 3.0 beta	Free. Install. Beta. version.	Personal data management. Cookie filter. Spyware filters. Access control.	Collection limitation / choice. Notice.	individual.
YOUPowered www.youpowered.com	privacy/security/marketing services company ??	?	Yes	United States	SmartPrivacy Publisher	Pay. Install.	Personal data management.	Notice.	organisation.
Zero Knowledge www.zeroknowledge.com	privacy/security company	1997	Yes	Canada	Freedom Internet Privacy Suite v. 2.0	Free / pay. Install. Free for standard / pay for premium.	Anonymity / pseudonymity. Cookie filter. Ad filters. Spyware filters. Mail privacy.	Security. Collection limitation / choice. Collection avoidance.	individual.
ZipLip, Inc www.ziplip.com	privacy/security company	1999	Yes	United States	ZipLip Plus	Free. Registration required. Web based.	Encryption. Anonymity / pseudonymity. Mail privacy.	Security. Collection avoidance.	individual.

ANNEX II: CAN WE BE PERSUADED TO BECOME PET-LOVERS?*

Introduction

Over the last decade and a half, the community of data protection regulators, technologists interested in privacy and others have developed both the concept and the tools of privacy-enhancing technologies.¹

By privacy-enhancing technologies, we may understand those digital systems, as used by and embedded in products and services, that attempt to limit risks to privacy and support the exercise of data subjects' claims to privacy, including those that attempt to control the processing of personal information in ways that reduce the risks of illegitimate processing, for example, by supporting claims to anonymity or pseudonymity, allowing data subjects to express preferences about the use of their information and to obtain secure access to what is held on them, supporting consent to collection or processing, limiting what is collected or how or to which systems it may be disclosed, and so on.² This is a wider definition than some people's: I do not confine privacy-enhancing technologies just to those tools that provide pseudonymity. Moreover, I do not here use a distinction between privacy-enhancing and privacy-enabling tools: I use the same term to cover both. At the appropriate point in the argument, a taxonomy will be offered (see Figure 3 below). In the present sense, however, privacy-enhancing technologies are one of the informational equivalents of the plethora of safety devices which are increasingly designed into everything from chemical and nuclear power plants to airliners.³

This community is now interested in the questions of whether businesses can be persuaded to invest in them, and whether consumers can be persuaded to demand them. Hitherto, such information as we have about the extent to which on-line businesses now offer even the simplest privacy practices such as providing information about collection, use and disclosure, offering choice about what information consumers might reveal or over disclosures, and subject access, suggests that only minorities of businesses have made even these modest investments.⁴ Proportions offering pseudonymity are almost certainly much lower. Indeed, one academic study soon to be reported involved using a personal computer equipped with the new IE6 software, including the P3P privacy preference definition system, to visit a number of commercial Websites: the study found that the researcher was asked by a significant proportion of the sampled sites' software to downgrade her privacy preferences in order to use the site.⁵ This suggests that if governments want to see wider use of privacy-enhancing technologies, there is a need for some persuading to be done.

I use the word, "persuasion", quite conscious that I am being indelicate. Hitherto, the OECD has, quite understandably, preferred to speak of "education", which sounds much less invasive and manipulative. For although — and no doubt in part *because* — we live in an age which considers that its arts and capabilities

* This study was prepared by Dr. Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London, in his capacity as a consultant for the OECD. The author is grateful to Anne Carblanc of the OECD for commissioning this paper, and to Anne Carblanc, Charles Raab, Phil Boyd, Brendon Swedlow, James Tansey and Mary Culnan for their comments on an earlier draft. The author feels that none of these people should be thought necessarily to agree with his arguments, still less do they bear any responsibility for his errors.

of persuasion have been developed quite remarkably exquisitely, it is now considered indecorous to admit that persuasion is indeed what is being done in the name of communication, education, training, the provision of information, and even in advertising. Nevertheless, in trying to assist the OECD in thinking about the question of when, for whom and under what circumstances “communication” about privacy-enhancing technologies (PETs, from now on) might actually work, in the sense of inducing people to be more willing to use them, it is impossible to avoid acknowledging that persuasion and influence are the point of the exercise. Indeed, much of the work on which it is necessary to draw in this paper is explicitly concerned with persuasion. I have no space here to discuss the spectra of more and less invasive, and more and less manipulative forms and strategies of persuasion. However, it is worth noting that those who have researched propaganda of various kinds have generally concluded that the more manipulative and the more insidious strategies are often ineffective, at best tend only to work in the short term, and as their true character emerges over time, tend to be self-undermining.⁶ I shall therefore assume that we are interested in how far the more honest ways to seize hearts and minds might be deployed to stir up motivation to use PETs.

My argument will be that not everyone is equally open to persuasion about anything, still less about everything, but that we can say something about who might be more open to persuasion about what and under which circumstances, and we can say something — albeit a little more modestly — about how differently situated people might be persuaded about the things they may be open to persuasion about. However, classifying and segmenting businesses and consumers is the key to understanding what can be achieved with people in different situations. This is, I know, an annoying conclusion for those who are looking for something more “can do”. The one kind of advice that, since the screening of “Yes, Prime Minister”, civil service policy advisors now try to avoid is anything that smacks of Sir Humphrey’s phrase, “It’s all very complicated, Prime Minister”. Unfortunately, sometimes, it just is. I shall, however, try to simplify and show that there is order in the complexity of just who is open to persuasion about what.

Contrary to the prevailing wisdom of the less socially oriented psychologists who have dominated the debates about both political and commercial persuasion for a century now, I shall suggest that looking at mental factors will not help us very much: that approach does little more than describe the shape of the problem to be understood. On the contrary, I shall argue that, in the words of one of the greatest studies of who persuades whom, why and how in the last half century, “where you stand depends on where you sit”.⁷ That is, the openness to persuasion of both businesses and consumers is explained largely by their situation, for it is location in institutional context that determines what information one can hear, accept and use and what information one will reject.⁸ Nor indeed is a simple approach of offering incentives enough to open people to persuasion, and, indeed, as I shall note below, many economists are now recognising this too. Incentives may have their place: but not everyone counts the same thing as an incentive, or at least, as an incentive worth having.

The paper has a very simple structure. The next section sets out a short characterisation of the nature of the problem to be tackled. Then there follow two substantive sections that present an account of the openness, first, of businesses, and then, secondly, of consumers, to persuasion, respectively to offer and to demand services in which PETs are used or embedded to protect privacy. In each of these sections, the same strategy is employed. The argument begins with an attempt to segment the populations of businesses and consumers in relevant ways. The analysis of segmentation is then used to identify which kinds of privacy protections would be expected to be of greatest interest in each segment. In each, a short subsection then discusses the means by which persuasion might be applied. These two central elements of the argument are followed by a final substantive section which shows that the basic approaches used in respect of businesses and consumers are not only compatible, but are in fact identical in underlying structure, even though this may not have been obvious at first sight. This enables a discussion of the dynamics of interest in and openness to persuasion about PETs in which I examine consumers and suppliers in the same frame. A short

concluding section summarises the main lessons for public policy makers who want to try to persuade businesses and consumers to show more interest in PETs.

The structure of the problem of persuasion and what we need to learn

Offering consumers products and services designed using privacy-enhancing technologies (PETs) requires investment by businesses, and businesses are only willing to incur the costs of investment if they believe that it will be sufficiently profitable to do so. In many situations where PETs are retrofitted into information systems — though, of course, by no means all — the effect is to increase unit costs. The effect may be much less for new products that are designed from the beginning to use PETs. If companies fear that they cannot pass on those additional costs in the form of higher prices, then they will fear that their rivals will be able to undercut them by offering services and systems that do not feature PETs. The direct benefits of privacy redound to consumers (and perhaps to wider publics), not to the businesses: for businesses, the benefits are indirect. The problem of persuading businesses to invest in PETs, then, is a conventional one, like that of attempting to induce them to behave ethically, or to adopt environmentally beneficial practices. To put the problem in economic terms, the challenge is to persuade businesses that they should internalise certain costs that they have been able to externalise, where market competitive conditions might — at least in many markets — favour those who externalise over those who internalise.⁹ This is not, as I shall show, necessarily an insoluble problem, but it does represent a challenge, to which there are only a finite number of basic types of response. However, to learn something about those types of available response, we can look to the lessons from attempts to influence businesses to adopt environmentally beneficial technologies, or to behave ethically in a variety of ways, and we can consider whether there are lessons for the situation in respect of PETs.

To make this paper manageable, I am going to ignore the problem of persuading government agencies, either providing services or purchasing them from the private sector, to adopt PETs in their service specification.¹⁰

Now consider the nature of the challenge of persuading consumers to demand PETs. The key issue is the nature of consumer preferences. Not all consumers care to the same degree about privacy: some care about some privacy risks more than they care about others, some have more faith in the efficacy of technological protections against privacy risks than others and some have more faith in some technologies than in others. This means that the first thing we need to understand is how consumers are distributed in terms of their *risk perception* about a variety of privacy risks. That is to say, recognition of risk drives consumers' desire for protection. Moreover, in order to understand the scope for persuasion, we need to know how open to influence and change risk perceptions about privacy are.

In a market in which the price charged for those products and services in which PETs are embedded is higher than the price of those in which they are not (a “worst case” assumption that we can well follow in order to make the argument most widely useful), the consumer must decide how much (s)he values the kinds of privacy that the service offers protection for, against the actual size and cost of the price increment. The second thing we need to learn about consumers, then, is how preferences for protection against various kinds of privacy risk are *traded off* against price increments. If these trade-offs are to be influenced, presumably then (unless someone has a new idea about how to increase consumers' levels of discretionary income without causing corresponding price inflation!) the only way in which to persuade people to be willing to pay more for privacy protection is to increase the seriousness with which they take privacy risk in the first place.

In the unlikely event that the market were perfectly competitive and consumers could (nearly) costlessly find and move between suppliers, consumers would sort themselves by their preferences and their

willingness to pay for goods and services according to the trade-offs between privacy “quality” and price that they are prepared to make, with the information that they can (in a perfectly competitive market) acquire about the privacy protecting characteristics of rival services at negligible cost. In many real markets, of course, there are real costs for consumers of search, information acquisition and checking and of exercising mobility between suppliers — further there may be oligopoly or other limitations upon the range of services available to be chosen between, and companies may offer misleading information about the privacy-protecting characteristics of their services. The third thing, then, that we need to learn about, is how consumers value the *transaction costs* — which may not all be monetised, but may be expressed in terms of lost time — of search, checking and mobility.

Persuading businesses

Why should businesses internalise costs that they might otherwise externalise, and that they might fear that their competitors might externalise if they internalise them? In general, there are four basic types of situation in which businesses might have reasons to do this which can be grouped under two general headings. The first group consists in situations in which businesses are given *sanctions* and *incentives* to internalise those costs, and the second comprises situations where there are *constraints* upon them that make it difficult for them to think of choosing not to internalise the costs.

Sanctions and incentives

1. *Fear*: Here, businesses fear that if they do not internalise the costs and invest in PETs, they will face sanctions from regulators. If there are standards for PETs created by national and international standards bodies, for example, they will adopt those standards because the standards can be used in signalling to the regulators that they are acting in the ways that regulators demand, and so they can create a reputation with regulators for their commitment to the values for which the regulators call.
2. *Hope*: In this situation, at least some groups of consumers of importance to the business demand PETs in the design of their services or products, and therefore investment in PETs can represent competitive advantage vis-à-vis rival firms in seeking the business of those groups of consumers. Here, adopting PETs standards serves a signalling function toward and helps to create a reputation with those groups of consumers.

Constraints

1. *Habit*: In this situation, for businesses within a particular industry or niche in that industry, the use of PETs has become the norm, and, independently of any incentives or sanctions, they are adopted and the costs internalised because all competitors do this as a matter of implicit routine, and they are no longer conceived as a separate issue. The habit in effect limits the “thinkability” of not using them.
2. *Unavoidability*: Here, PETs become embedded in other products and services that have to be used because there are no alternatives to using at least one of them. For example, product standards might specify PETs have, in this situation, become universally adopted. Typically, this situation arises in cases of technological path-dependency, where, independently of any competitive advantage or regulatory pressure, certain technologies achieve “lock-in” — to use some other systems becomes impossible in part because the power of expectations and the power of costs of change for businesses and consumers are now too great, so institutionalised has the technology become and so established is the infrastructure around it.¹¹

For the present purposes, we must — unfortunately — ignore habit and unavoidability, for as historical studies on the lock-in of the QWERTY keyboard and the internal combustion engine have shown, there is no direct route to the habituation or unavoidable ubiquity of a technology that does not first pass through the dynamic pressures of hope and fear. All habits and innovations are new at some point, and to survive the “liability of newness”, they must be adopted explicitly at first and on the basis of some balance of hope and fear.

However, situations in which hope and fear can motivate the internalisation of costs that rivals might externalise are not universal, but are to be found in quite distinct types of sectors. For the same reasons that explain their particular distribution, combining the powers of hope and fear is also far from straightforward.

Consider situations first in which fear of regulatory sanctions is most likely to be effective. Regulators are, of course, most effective in the most regulatable sectors of the economy. These are typically the most stable, because the costs to regulators of acquiring information about such free riding behaviour as exploitation of consumers’ privacy are very great in highly volatile, highly competitive sectors.¹² Moreover, in markets and sectors where companies appear, disappear and reappear in new guises with bewildering speed, enforcement is difficult for regulators.

In those market sectors where consumers cannot readily know whether their privacy is being respected, perhaps because they are not aware that those industries possess much information about them (or perhaps because they are not aware that certain kinds of information about themselves is in fact highly valuable, because it may provide excellent predictors of other kinds of information), there are many more opportunities for firms to exploit personal information unscrupulously without the detection of regulators who often rely upon consumers to alert them of violations.

Markets and sectors differ in the degree to which they exhibit institutionalised arrangements for sharing information around the market about what other firms are doing to create good and bad reputations for firms and for senior executives. Those sectors without such institutionalised information sharing systems offer more opportunities to the less scrupulous firms to evade the not-so-long arm of the regulator.

However, the economic characteristics of markets are not the only features that make for ease of regulation. The degree of scrutiny by pressure groups including consumer pressure groups concerned with privacy issues also matters. Those industries to which these groups choose to devote their scarce resources are thereby made easier to regulate, because the pressure groups bear some of the costs of acquiring information that would otherwise fall to regulators.

The internal institutionalised characteristics of firms also matter greatly. Firms where leaders are committed to consumer privacy are more likely to have institutionalised controls to ensure that PETs are used, to support whistleblowers who would report violations, and to be willing to co-operate with regulatory requests for information. However, these institutionalised characteristics are not randomly distributed: commitment to such controls will appear where it makes sense to do so, and this sense-making differs according to context, including market niche.¹³

Now consider those sectors in which hope-based strategies might work to discipline businesses to invest in PETs. Hope rests essentially on consumer demand, which we shall consider in more detail in the next section. However, whatever one’s account of how consumers differ from one another in the importance they attach to privacy in general, and to protection against different particular privacy risks, it is generally recognised that some consumers have preferences that, if businesses can profitably attract those consumers, might leave those businesses more open to persuasion that PETs are worth investing in than otherwise. The key questions for hope-based strategies are these: how big is the constituency of consumers who want any

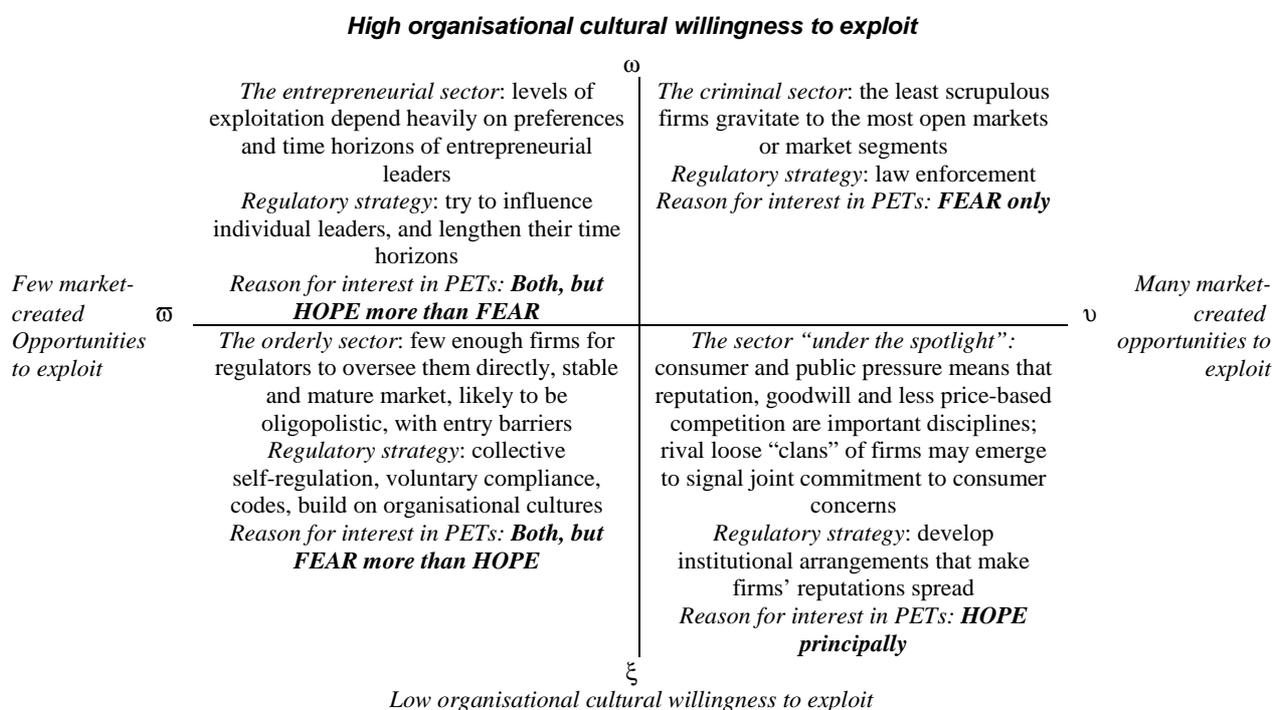
of the available kinds of PETs, how much are they prepared to pay, and how costly will it be for businesses to attract them?

The field of environmentally sensitive consumption may provide a good analogy here. Research on the “green consumer” trend, and on the take-up of composting of household organic waste, recycling, use of “fair trade” coffee and tea, minimal packaging, willingness to use organic whole food co-operatives for groceries, and other environmentally protective consumption behaviours has shown that these are classical niche markets. That is to say, a modest number of people with very intense preferences can sustain a small market with many small firms, but there are limits to the scope that these markets exhibit for growth, because although other consumers would be interested in some of these products, either the price differential puts them out of their reach, or the transaction costs of time and effort are too great.¹⁴ Unless these products represent good value for money, and unless environmental preferences are very strong, demand is limited, and even modest price incentives have only marginal effects.¹⁵ Just occasionally demand for such products can be increased by powerful marketing, where a large and powerfully branded company is prepared to adopt these products as a way to internalise the costs. For example, supermarket chains in the United Kingdom and continental Europe have expanded demand for GMO-free and organic foods, at least for a while, but even here they have had difficulty in sustaining this, and households on lower income still find these products unaffordable. Research on “buycotts” — that is to say, positive campaigns by consumers with very intense preferences to buy only goods and services where suppliers have internalised certain costs to offer desired features even at a premium — suggests that they are few in number,¹⁶ that they rarely work in eliciting positive supply response on a really large scale without powerful backing of fear-based factors such as the regulatory action to prohibit alternatives,¹⁷ and that they are very difficult to sustain especially where demand is essentially niched and where there is an unfavourable price differential.

This suggests that the key question about services with PETs is whether demand for privacy is like demand for eco-friendly products, or whether it is something that attracts wider consumer commitment, especially where there are unfavourable price differentials between services using PETs and those which do not. I shall consider the evidence in more detail in the next section, but most surveys suggest that very intense preferences for privacy that lead consumers to be willing to pay price premia over prolonged periods are probably a minority taste in most countries, but that there are certain goods and services around which those preferences cluster more than others. In particular, because so many people regard as uniquely “sensitive” data about their health and their finances, there may be more widespread willingness to pay a premium for services using PETs in such industries as financial services, insurance and medical care than elsewhere.

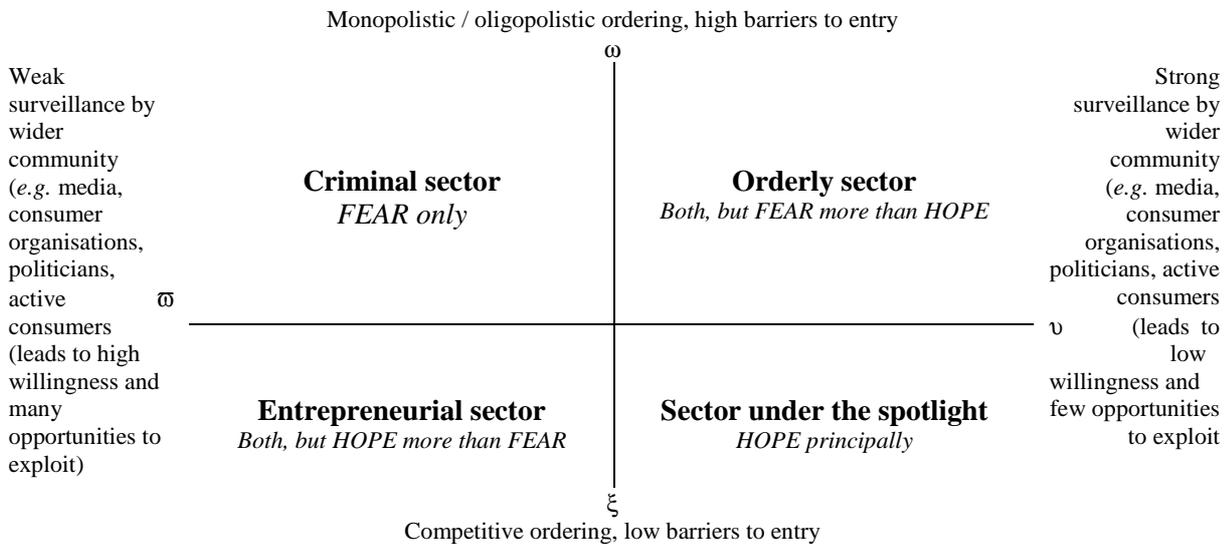
These are all simply cases of the problem of persuading companies to internalise costs that they fear their rivals might gain competitive advantage by externalising, and the balance of hope and fear in that persuasion. A good summary of this argument that the drivers of fear and hope (that might lead companies to internalise costs that they might fear that their rivals might externalise) are unevenly distributed across the economy, is provided by the business economist S. Prakash Sethi, writing with Linda Sama.¹⁸ In their account of the differential pressures on business to behave ethically, quite generally, Sethi and Sama identify a number of strategies for regulators seeking to persuade businesses to internalise costs, that might make sense in each of these situations. Figure 1 below is, I hope, a reasonably faithful gloss or adaptation of their graphical representation of this analysis of the problem, although the titles of some of the sectors and the balancing of hope and fear factors are my own.¹⁹ These authors structure the nature of these different situations along two intersecting dimensions describing the distribution of incentives. These two dimensions are the degree to which organisations’ own internal institutions militate against consumer exploitation and the degree to which the organisation of the market creates opportunities for exploitation.

Figure 1. The institutional situation of businesses shapes their openness to persuasion
(adapted from Sethi and Sama, 1998, 93)



It will be important for the argument in the next section to see that this matrix can be rearranged, using slightly different dimensions. The extent of opportunity and the extent of willingness to exploit are not settled or caused wholly independently, on institutionalist accounts of the origins of preferences: indeed, willingness and preferences often emerge and become definite partly in response to what are perceived as opportunities.²⁰ Behind both of the two Sethi and Sama dimensions is the extent to which surveillance by the wider community disciplines both the ability and the willingness of businesses to exploit, for it is in the sectors in which there is less surveillance due to the costs of its exercise, that the least scrupulous gravitate, and where they are cultivated, for the sense of being under surveillance acts as an institutional pressure that induces willingness to restrict exploitation and that limits opportunities. Now, we can helpfully introduce a dimension that is implicit in the Sethi and Sama analysis, namely, the degree to which the market ordering is structured by monopoly or oligopoly with barriers to entry — creating something akin to a kind of authority within the market — at one end of the spectrum, and, at the other, the degree to which it is organised by relative openness to competition with free barriers to entry. This measure of the structure of markets also indicates the nature of the ways in which surveillance is mediated. Where there is oligopoly and there are high barriers to entry, direct consumer power is attenuated; conversely, where there is greater openness, direct consumer power can — depending on the other variable of surveillance — have more weight. Cross-tabulating these two dimensions enables us to produce exactly the same analysis of sectors as Sethi and Sama. However, rearranging the matrix in this way will turn out to be very important in examining the relationship between the differential openness of differently situated businesses to persuasion and the differential openness of differently situated consumers, for it will enable us to map the situation of businesses in a way exactly comparable to that which will be introduced for consumers. This transposition of the classification of situations that make for differential openness to persuasion, yields Figure 2.

Figure 2. Transposition of Figure 1



What kinds of PETs are firms in each of these sectors of the economy (faced with these structural pressures from the market, consumers and wider publics and regulators) most likely to be open to persuasion to using?

In order to answer this question, we need a classification of PETs, in the wide sense used in this paper and defined in the introduction. There are of course a great many in use, but for the present purpose, we need a classification by function — that is to say, by the category of risk against which the PET offers protection — rather than by technological type.²¹ For it is function that is of the first concern to businesses, although cost will of course come a close second. Figure 3 presents such a functional classification.

The next stage in the argument is to work out what the relative cost implications of each type of PET might be. What matters here is not the initial purchase price, but the long run economic costs of running a data management system subject to the constraints that a type of PET imposes, where one examines the implications for the basic business model as well as the implications for administrative costs. It is not possible to say very much about relative differentials in the long run projected costs of technologies that would perform these tasks, since over the medium term those costs are in part dependent on the level of demand for them: greater demand would typically in the short term increase prices, but as supply response builds up and as investment costs are recouped, prices are likely to fall in the medium to long term. Cost over the long run is in part a function of the size of the customer base, the value of the services in which the PETs are embedded, and the longevity and value of the relationship with the consumer. However, it seems reasonable to suppose that, in the short run, those systems that involve the greatest change to existing data management practices are the ones that are most likely to represent the highest total costs to businesses. Over the long run, the integrity of the data set (its adequacy in covering the people the business wants to reach, and the consistency of the data held about each person) determines the use that can be made of it. Therefore, when PETs impact on these things, we should expect the greatest true economic (opportunity) costs to arise from them, even if the greatest cash accounting costs do not show up here.

Figure 3. Functional classification of types of privacy-enhancing technologies (PETs)

PETs might be designed to carry out any of the following functions:	
1.	<i>Notification</i> : provide for notification of collection, identity of data controller, nature of use, disclosure etc.
2.	<p><i>Consent</i>: allow for consent prior to collection by:</p> <ul style="list-style-type: none"> a. Opt-in, or by b. Opt-out mechanism. <p>Which may be for:</p> <ul style="list-style-type: none"> i. Any collection. ii. Collection of defined categories (e.g. categories deemed particularly “sensitive”).
3.	<i>Collection type limitation</i> : limit quantity or type of information collected by some rule independent of consent, and typically by some coding which is defined by the legitimate purpose.
4.	<i>Collection context limitation</i> : limit contexts in which information can be collected to those falling under defined descriptions (defined independently of consent, and perhaps by legitimate purpose).
5.	<i>Subject access</i> : allow subject access.
6.	<p><i>Data change opportunity</i>: allow subject access and</p> <ul style="list-style-type: none"> a. Request for correction. b. Request for deletion of excessive and irrelevant information. c. Request for complete deletion of their individual record.
7.	<p><i>Alerting</i>: introduce “tripwires” in the use of information e.g. “stop and think”, “stop and check” instructions before using information:</p> <ul style="list-style-type: none"> a. For certain purposes. b. To carry out certain types of inference e.g. about derived classifications, marked as suspect for certain offences.
8.	<i>Identification limitation</i> : limit identifying presentation: i.e. limit capability to identify the individual from the information available to non-authorised persons through the use of pseudonymity, and/or blocking out of other key collected information.
9.	<i>Destination limitation</i> : limit by rule the possibilities of disclosure destination, e.g. prevention of copying of data.
10.	<i>Information</i> : notify data subject of rules, codes, etc. accepted by data controllers governing collection, purpose, actual uses, disclosure, and of any available redress, internally or to public regulatory authorities.

On this basis, therefore, we should expect that the cheaper PETs to implement will be those that would provide staff with alerting (7), or that would provide consumers with information (10). These involve no major changes to standard designs of databases. Into the next band might fall subject access systems (5) and those that would provide individual level notification (1). Secure on-line real time subject access is expensive, but when many more services are being provided online in any case, the marginal additional cost may typically not be too great. Identification presentation limiting systems (8) may be costly to retrofit, but are negligibly more costly to design into new systems, and not always particularly expensive to operate thereafter, depending on just who is locked out of identifying information and how much

inconvenience this causes them. However, this does involve substantial additional complexity in the basic design of a database, and in the rules governing retrieval and reports that can be run upon it, *etc.* Systems that allow individual level data change requests (6) are costly to operate, because they involve a lot of individual record level work some of which cannot be fully automated, although it can reduce other costs that would arise from inaccuracy (although secure real-time online subject access involves individual level display, it does not involve individual level authorisation for change). Most expensive are those technologies that could threaten the coverage of the database that a company wants to assemble — such as technologies supporting consent (2), limitation of collection (3) and (4) — and those that could disrupt plans for commercial relationships — such as destination limitation (9). Figure 4 summarises this very rough hypothesised banding. I accept, of course, that this is very rough and very provisional. However, if a better banding can be offered, it could be used in much the same way as this will be used in the argument that follows, without disrupting the basic argument of the paper.

Figure 4. Suggested rough cost bands for PETs

Band	Type of PET
A: cheapest	7: alerting, 10: information
B	5: subject access, 1: notification
C	8: identification presentation limitation
D	6: data change request
E: most expensive	2: consent, 3, 4: collection limitation, 9: destination limitation

To some extent, it is clear, the hot breath of consumer preferences on the necks of companies in different sectors will shape their openness to persuasion to invest in different kinds of PETs. These will be examined in detail in the next section: however, for the present, the following assumptions can reasonably be made.

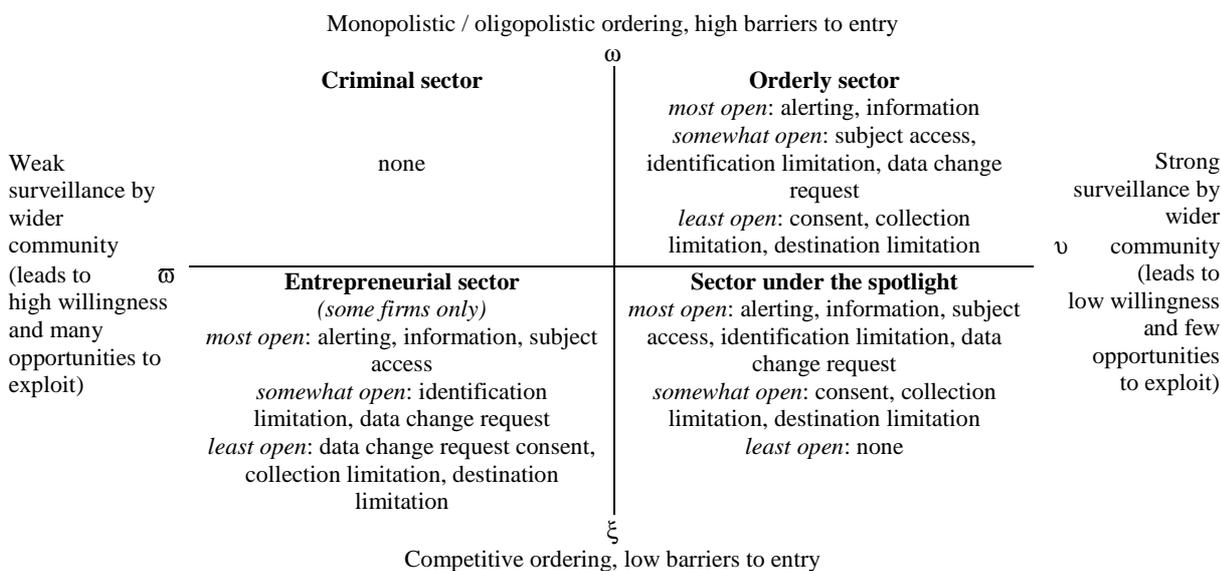
- a. *Criminal sector*: Here “criminal” is a term of art: we are concerned only with those firms that unscrupulously ignore privacy. Many businesses supplying illegal products are highly responsive to consumer preferences about both products and privacy: illegal businesses supplying illicit drugs are highly responsive to changes in tastes for drugs and respect consumers’ privacy very carefully. However, the present concern is only with businesses prepared to use methods of personal data handling that are illegal, so in this sector, by definition, consumer preferences specifically for privacy have little impact. Such firms may well of course not be engaged in any other illegal activity.
- b. *Orderly sector*: Here consumer preferences are quite powerful, but the stability and oligopolistic nature of the market mean that they are often more powerfully refracted through regulatory action (fear) than directly (hope).
- c. *Entrepreneurial sector*: Here firms are small and mobile enough to be able to sort themselves according to their understanding of the segmentation of consumers, and so those that want to respond to those consumers with strong privacy preferences will find ways to situate themselves to signal their responsiveness to those consumers, and those which are less scrupulous will search for niches where either they can serve consumers less concerned about their privacy, or else where their data handling practices will not be so obvious to consumers.
- d. *Sector under the spotlight*: Here consumer preferences about privacy are likely to be at their most powerful, and most powerfully amplified through consumer and human rights movements, as well as influencing ways in which regulators allocate their attention. The ways in which firms will form

loose “clans”²² — using, for example, trust seals (such as BBB Online, Truste™ and Trust UK) — to display their joint commitment to privacy issues, will also provide consumers with important signals and “hostages”, increasing their exposure to consumer privacy preferences.

Trade associations may act as forces for compliance with privacy standards and for the use of PETs, sometimes almost as regulators, and sometimes as “clans”. In either of these cases, however, we should expect their ability to attract members to be greatest in the orderly sector and in the sector under the spotlight. Ideally, one might want such trade associations to be most effective in the small and medium-sized enterprise sectors — which would be distributed between the entrepreneurial sector and the sector “under the spotlight” — for these firms are the ones likely to have the fewest resources to afford the costs of search, evaluation, adoption and learning the use of PETs. However, their ability to attract members in the entrepreneurial sector is typically lower, for here the competitive pressure of fear that rivals will externalise costs is greatest.

Taking together these considerations of the different functions PETs can serve, suggested bandings of cost differentials and the different pressures that firms in the four different sectors face, we can offer the following hypothesis as to which sectors will feature firms most open and least open to persuasion about each type of PET. The key issue is how far down the hierarchy of costs bands for PETs businesses in each situation might be prepared to go. Figure 5 sets out the hypothesis that emerges from the application of the framework set out in Figure 2 to the cost banding set out in Figure 4.

Figure 5. Relative openness to persuasion to invest in types of PETs by sector



Note: In this Figure, “most / somewhat / least open” means “most / somewhat / least open to persuasion to invest in the following types of PETs” by comparison with *other types of PETs*. I assume that the cost bandings between types of PETs set out in Figure 4 are the same between sectors, and so the general ordering is the same. However, in some sectors, the willingness to internalise the costs of the most expensive costs bands of PETs should be expected, on this account, to be greater than in other sectors.

If the argument so far is accepted, then what does it suggest should be the strategy of data protection regulators, government departments with policy responsibility for oversight of the business community’s data management practices, and for consumer and human rights social movements concerned with privacy in the commercial sector, and self-regulatory bodies ranging from trade associations through to privacy seal bodies, in attempting to persuade businesses to invest in PETs?

The first strategic issue is whether to focus scarce resources available for persuasion upon the businesses that are easiest to persuade — which are of course likely to be the ones least likely to exploit consumers in any case — or on the most difficult to persuade. In theory, this is a difficult social policy choice because it requires the balancing of urgency against feasibility, but in practice, government bodies invariably decide on the first course of action: feasibility wins every time. Politically, the imperative to show “quick wins”, the need to build up skills in persuasion and capabilities in gathering information from those being persuaded, and the fact that in a developed country with a basically law-governed system of capitalism, larger numbers of firms are open to some persuasion, means that there is little choice but to focus on those who are easiest to persuade, even though the worst risks arise in connection with the most difficult to persuade. It is on this assumption, presumably, that Sethi and Sama’s general advice to regulators is based (see Figure 1).

As Sethi and Sama note, with the criminal sector, the only really persuasive force is law enforcement: here, hope has little grip and fear is the only persuasive tool available to government agencies.

There has been a great deal of development of formal training programmes for businesses in privacy protection: law firms, management consulting houses, privacy trust seal groups, professional networks of chief privacy officers and dedicated specialist data protection consulting advisory agencies have developed such programmes in many countries. The account of openness to persuasion offered here would suggest that these formal training structures are most likely to be of use in the *orderly* sector, where stable market shares, mature markets and technologies and hierarchical and bureaucratic systems of data management are most likely to be found. Secondly, these means of persuasion should attract at least some interest in the sector *under the spotlight*, where specialist compliance officer roles may not be expected to exist, but where a variety of personnel with data management roles might be attracted by formal training. The greater interest of these sectors in such support follows from their greater exposure to surveillance. However, in the entrepreneurial sector, this rather bureaucratic approach is much less likely to be successful. If there is interest in these training programmes from the criminal sector, it will usually be from law firms that act for these companies or else from managers interested only in using what they learn on such courses to work out better ways of disguising their sharp practices.

With firms in the *entrepreneurial* sector and perhaps some in the small-firm-dominated industries in the sector *under the spotlight*, much more informal techniques of delivering information for persuasion are more likely to be effective than formal training. In the entrepreneurial sector, we would expect that looser, more individualistic structures such as casual networks would be more appropriate. These may have some appeal in some parts of the sector under the spotlight, but in that area, working through the clan-like systems to develop commitment to PETs as part of the “membership criteria” for trust seal clubs and other reputation-enhancing and consumer-signalling institutions is more likely to be effective.

PETs could perhaps be introduced, as it were, by stealth, by marketing a technology and tool to businesses purely on the basis of its data processing functionality, so that its introduction does not alarm those businesses that might otherwise be concerned about the cost implications of supporting consumer privacy, by suggesting that these are simply the normal running costs of handling data about consumers. This is achieved by embedding PETs in a variety of products without necessarily making a great deal of noise about the privacy-enhancing aspects. The aspiration behind these strategies is to obviate the need for persuasion in order, it is hoped, to proceed directly to unavailability or at least habit. It is, I have noted above, unlikely that such manipulative techniques are likely to be successful for very long. However, this is a very different thing from routine creation of agreed product and process standards through the national, European and international standards authorities for management, organisational and operational processes for ensuring best practice in data protection privacy including the use of PETs. This has been extensively debated at European level, but appears to be on ice at least for the time being, due to business opposition.²³ However, the Canadian Standards Association adopted such a standard in 1996 - (in Canada, unlike other

countries, it appears that the small business lobby appears sometimes willing to support regulation that their counterparts elsewhere would not, where they believe that it helps create a more level playing field between their members and big businesses). However, the decisions of at least the first businesses to adopt a proffered standard reflect persuasion: only when only the last few laggards are left on the conventional “S”-curve that economists use to model the rates of adoption of innovations,²⁴ can unavoidability be relied upon to secure adoption without persuasion. The development of PETs standards is something that should be understood, not as a persuasive strategy for regulators in its own right, but as a way of supporting the very different hope-based business strategies of firms in each of the three non-criminal sectors.

This completes the account offered in this paper of the openness of businesses to persuasion to internalise the costs of PETs that they might fear their rivals might externalise, the types of PETs each sector is structurally most open to persuasion about, and the means by which such persuasion might most effectively be delivered within each sector. The next section will examine the variations in the situations of consumers in order to explore how consumers and businesses in different situations face one another.

Persuading consumers

It was argued above that, in order to understand which consumers will want the kinds of privacy protection that embedded technologies can offer, we need to understand the differences between consumers in respect of their:

- *Risk perception*: differences between perceptions of privacy risk, and how open to influence those perceptions might be.
- *Price-sensitivity*: how preferences for privacy are traded off against price differences between services that use PETs and services that do not.
- *Transaction costs*: how consumers differ in their willingness to bear the sometimes non-monetary transaction costs of search, mobility between providers, and making available their own time and effort to use the privacy protections afforded (*e.g.* actually invoke subject access rights or request corrections), and how these might differ between market situations with more and less competition.

I have reviewed elsewhere the literature on privacy risk perception,²⁵ in order to argue that the conventional segmentation of the population into a small group of the “unconcerned”, a tiny group of privacy “fundamentalists” and a large group of privacy “pragmatists” is in fact seriously misleading.²⁶ In the first place, risk perceptions change according to context:²⁷ they are not the applications to privacy of stable underlying psychological types. Secondly, the category of pragmatism is too vague and too capacious to be a useful one (many surveys using this concept find between two thirds and three quarters of the population to fall under it!), and it tends to lead businesses into a misplaced complacency that they can always offer consumers enough that they will then cease to care about privacy issues. It is also a problem that this taxonomy bears no relationship to the ways in which we understand people to think about other risks or other consumption relationships and practices. It would be very odd indeed if people thought differently and sorted themselves quite differently in relation to concerns about their privacy from the ways in which they think and sort themselves in relation to almost any other concern. This taxonomy is also very static. It offers no way of thinking about how people’s responses might change as their relationship with businesses and government changes. Finally, it is a major weakness of the unconcerned-pragmatist-fundamentalist taxonomy that it offers no explanation of where these categories come from, or just why anyone might come to think about their privacy in one of these ways. “People’s mind sets are just like that” is not an explanation at all, still less one that is very helpful to regulators or to

businesses who want to understand who might be open to what kinds of persuasion about what kinds of risks, opportunities and safeguards.

If we are to look for an approach that recognises that there are shifts according to context (albeit that some shifts are much more difficult than others), that is more precise, that does not induce misguided complacency, that recognises dynamism, that is grounded in some explanation of risk perceptions come from, and that is better integrated with what we understand to drive the ways in which people think about other concerns, then it makes sense to look beyond psychology. For, although psychological research on the perception of risks can tell us quite a lot about the variety of biases we can observe,²⁸ it has mainly offered accounts of what are claimed to be typical heuristics, rather than ways of thinking about differences and distributions, and it has had rather little to say about which biases will be exhibited by which people in which circumstances.²⁹

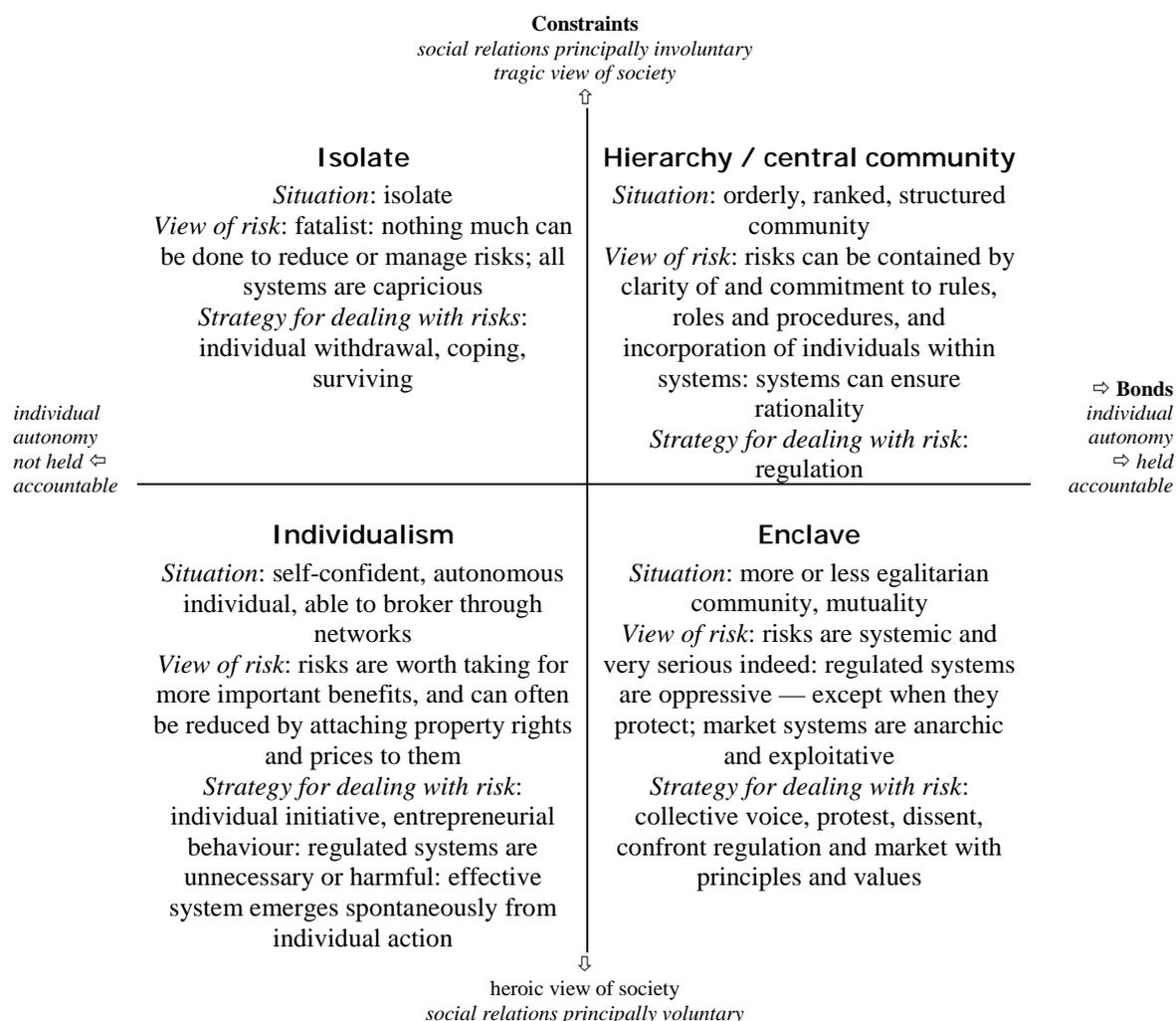
It makes more sense to begin with an understanding of where and how people are situated in social organisation, in order to explain the perception of risks.³⁰ However, there is not an indefinite variety to the basic forms of social situation in social organisation in which people can find themselves,³¹ and we can use a basic taxonomy of forms of social organisation to help us to understand how differences in risk perception about such things as privacy, will emerge and can be understood.

It may help to begin with some definitions of terms that will be used in this section to describe the situational factors that shape risk perception. By a person's "basic" or "primary situation", I mean the long term, underlying position that a person occupies in relation to the major institutionalised forces in their society, such as the labour market, the housing market, public services, key suppliers of goods and services, their peers as colleagues, friends and acquaintances, fundamental institutions such as religion, family organisation and the like. By "contexts", I mean the range of specific fields in which someone may yield up personal information about themselves, such as dealing with retailers, dealing with one's bank, dealing with one's physician, claiming a public service. It is the former which, on the view that I shall argue, is the really important factor, because it is this which shapes one's sense of identity, one's general outlook, one's capabilities, one's preferences and it does so by creating both constraints and opportunities and limiting accountability to institutions and to particular others. However, the primary situation is itself plural: we are differently situated in different contexts. For example, many of us have a quite different institutional relationship with our physician from that which we have with the supermarket we regularly use, and so we bring quite different thoughts styles to bear on our perception of privacy risk in relation to medical and retail data about us. By "secondary situation", I mean the much more short-run context of the particular conversations and interactions that a person may have with people who may deliberately or unintentionally try to persuade one to take a view of a privacy risk other than the view one would have, springing from one's primary situation. I shall argue that such psychological factors as personality traits tend to be shaped by the primary situation, modulated by context, rather than being independently caused and independently shaped by biases in the perception of risks.

Figure 6 presents a summary of the best-developed approach to understanding the perception of risks in general in recent social science. The figure presents a taxonomy of the basic varieties of primary situations which produce a basic and limited plurality of types of risk perception. This classification is produced by cross-tabulating two dimensions into a matrix. The dimensions are labelled using slightly more accessible descriptions of the two dimensions around which social science has circled since its inception. In 1897, Durkheim introduced these two concepts in order to understand how people's situation in social organisation shaped propensity to suicide. In "*Suicide*", he called what is here shown as the vertical axis, "social regulation", and what is here shown as the horizontal axis, "social integration".³² They have been given various names since then, such as "grid" and "group" by the theorist who first presented this matrix.³³ Cross-tabulating them yields four basic types of social organisation, all of which will spring up in any human society. The basic types recur in economics as markets (individualism), hierarchies and clans

(enclaves),³⁴ and the isolate category is widely recognised in sociology and anthropology.³⁵ Essentially, the matrix presents a set of hypotheses that have been successfully tested in a wide variety of research about the relationships between situations and thought styles about risk in general.

Figure 6. How situation shapes basic range of risk perceptions about any kind of risk



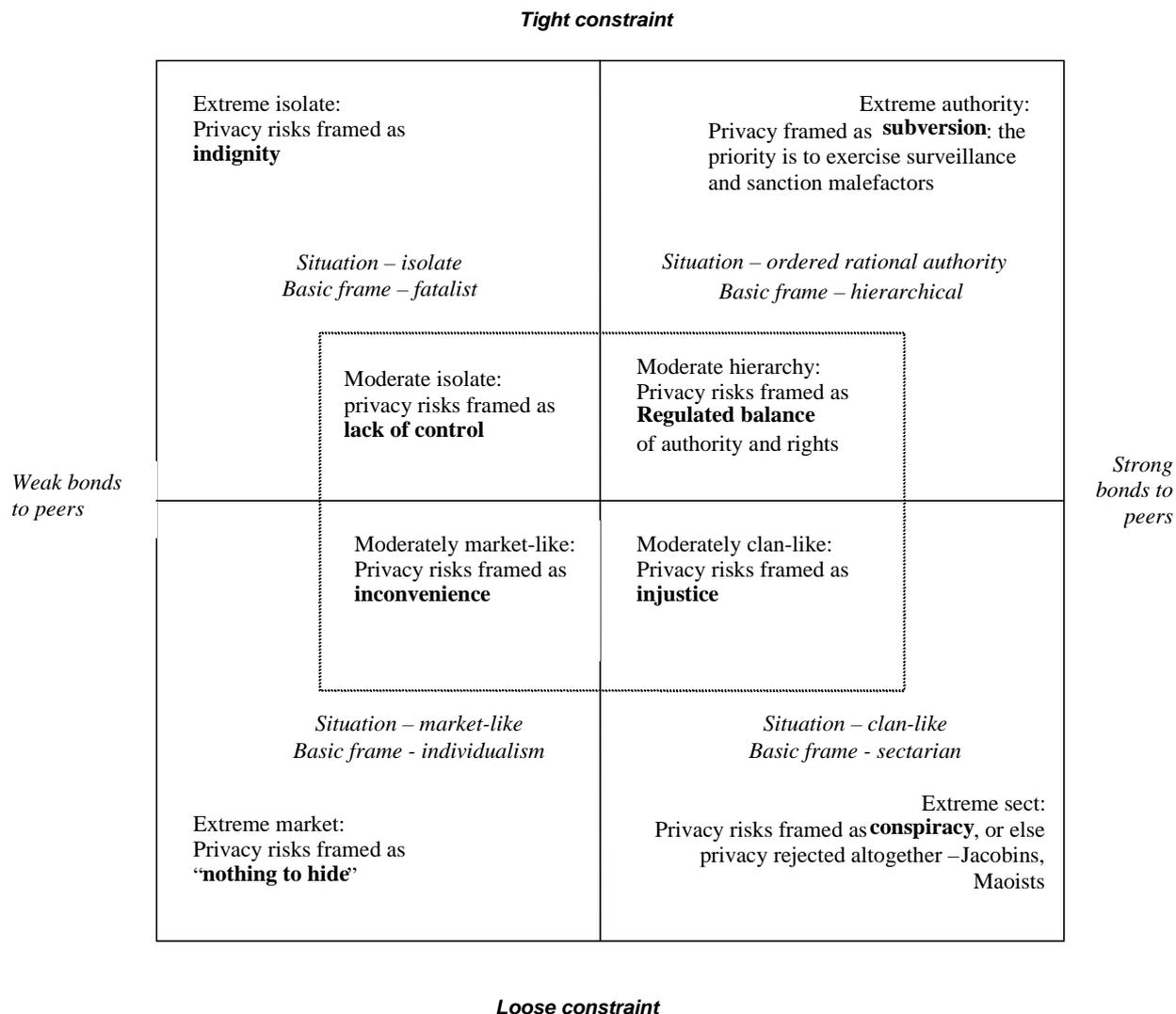
These four basic types can be found in the ways in which consumers think about privacy risk too. In a recent qualitative study conducted for the UK government, I presented the following application of the taxonomy, in order to explain the distribution of attitudes to privacy observed in connection with proposals for and practices of sharing of personal data between departments and agencies in the public services in order to promote “joined-up” or holistic government (Figure 7).³⁶ Within each of the four basic outlooks on risks, in the context of the focus group conversations, it was possible to distinguish more moderate and more extreme forms of the ways in which these basic outlooks applied to privacy risk. The application of the basic outlooks yields “frames”, or specific styles of thinking about privacy risk that are governed by an overarching concept.³⁷ Figure 7 provides a complete mapping of the eight available frames, produced by counting both the moderate and extreme forms of each of the four basic positions set out in Figure 6. Again, it should be remembered that many people will move between positions as they move between contexts.

In the study mentioned, the most socially excluded people, who were long term claimants of benefits, tended to be isolated and tended to exhibit the “indignity” in frame which they experienced data collection and data sharing as humiliating and demeaning, but as inevitable and part of the unavoidable fabric of life. The self-employed males, by contrast, who operated as brokers in networks, might sometimes begin with the “nothing to hide” frame, in which they would claim that no one with anything to hide need be concerned about privacy at all, but quickly shifted to the “inconvenience” frame, in which data collection and sharing was seen more as a nuisance than as a threat. Some of the older people who had grown up in the post-war years with their experience of commitment to a variety of solidaristic institutions in contexts such as health care, but who were now outside the labour market and its particular hierarchical rankings of status and had adopted a new identity as retired people with its sharply defined membership criterion, looked at privacy risks as matters of injustice, or as the violation by the state of general principles. The more extreme “conspiracy” frame tends to be associated mainly with privacy activist movements. Finally, the more hard-nosed members of the law enforcement community exhibit the frame in which they see privacy claims as subversive, insisting that without general surveillance, the control and prevention of crime would be impossible. More common among central civil servants, for example, who are charged with finding some settlement between the law enforcement authorities’ concerns and those of a range of wider publics, is a “regulated balance” frame,³⁸ in which it is hoped that some quasi-constitutional order can be defined and enacted in explicit rules that will reconcile the conflicting pressures in such a way that it can be administered by conventional administrative means.³⁹

It is not really meaningful to produce quantitative estimates of what proportions of the population might be described by each of these situations, precisely because there is such mobility in everyone’s life between contexts that constitute the cues for these situational dynamics. That is to say, the primary situation is itself plural for most of us. Many of us are prepared to be quite individualistic about taking a supermarket loyalty card with all the disclosure of personal information about our buying habits, yet feel much more enclaved about the way in which we want our primary care physician to manage the use and disclosure of our health records, while being content, deferentially to trust that some combination of regulatory oversight and professional codes will adequately govern the proper use by our bank of the data about our transactions on our accounts. This mobility reflects the plurality of our institutional relationships with large retail organisations, individual physicians and banks, as well as facts about the wider contextual aspects of our lives — education, religion, social networks, class, gender, and so on — that we bring to each of these contexts.⁴⁰ (This is not to say that people can or do make any move around this matrix with equal ease. As I shall show below, there are important differences in the height of the hurdles to be crossed between positions.) Although there have been attempts to produce estimates of an aggregate “worldview” bias using very general, context-free attitudinal statements in Likert scales (developed by the late Karl Dake) to measure individual positions within the taxonomy presented in Figure 6,⁴¹ precisely because these statements are so general and context-free, one has to have doubts about their meaningfulness, let alone the meaningfulness of attempts to draw cross-national comparisons.

If we had cross-nationally comparative data collected on differences in public perceptions of a variety of different types of privacy risk in specific contexts, that might be more useful. Still more useful would be cross-nationally comparative research that compared variations in perceptions of privacy risk both by context and by differences in primary situation. For this purpose, the survey techniques by Dake and his successors are only useful if they can be exactly correlated with information about people’s primary situation. There are some methodological approaches developed for doing this,⁴² but it has not been attempted to date.

Figure 7. How primary situation shapes the way consumers frame privacy risks



Because the perception of privacy risk is a key element in shaping interest in PETs, we should expect, all other things being equal, that people in each of these different situations will exhibit significant differences in the kinds of PETs, if any, that will be of greatest interest to them. The most fatalistic are unlikely to have much faith in either the efficacy or the relevance of most PETs to their lives. After prolonged periods of being at the informational mercy of large bureaucratic organisations, benefit claimants tended, in the study in which this analysis was refined, to feel that they have little chance of influencing, still less controlling the use of their personal information by those organisations by any technological means. The most cynical even doubted if they were able to see their records on-line, that the information that would be made available to them in the name of subject access would in fact be the true record. More moderate “lack of control” frames could be associated at least with a willingness to be interested in online subject access. Those with at least more moderate individualistic “inconvenience” frames tended to be interested, as we would expect, in those instruments that might provide some more individual access to their information, including the forms of consent that present the lowest barriers to any benefits that may come to them through the exchange of information — such as opt-out rather than opt-in consent systems. For them, information about the uses to which their data are put, is of most importance. Those with more enclave-type “injustice” frames, and certainly with more extreme social movement outlooks are much

more likely to be interested in technologies that limit data collections or that provide for anonymity or pseudonymity: indeed, the scale of data collection and the lack of anonymity *per se* has long been a central concern of social movements dedicated to organising for privacy.⁴³ Finally, those consumers with more hierarchical outlooks are more likely to be trusting of the agendas and rationales of large organisations as data controllers, and will therefore mainly want those PETs that enable them to correct minor errors, and at most may be willing to use some tools that provide pseudonymity in those fields where they feel that this is appropriate within the prevailing norms, more as a protection against other individuals than against abuse by large regulated organisations, in the procedures of which they have at least provisional trust. For this group, the existence of a law expressing a commitment to a social value — for example, data protection law — has a symbolic power that gives weight to that value.⁴⁴ Figure 8 summarises what we should expect.

Figure 8. What PETs might consumers with different patterns of risk perception be most interested in?

<i>Constraints</i>	
<i>Fatalism</i>	<i>Hierarchy</i>
? subject access	1. alerting, information 2. subject access, data change opportunity 3.? identification limitation
<i>Individualism</i>	<i>Enclave</i>
1. subject access, data change opportunity 2. consent by opt-out 3. information	1. consent by opt-in, collection type limitation, collection context limitation, identification limitation, destination limitation, notification 2. subject access

∪ Bonds

If we accept then that this provides a reasonable guide to the range of ways in which consumers perceive privacy risk, then we can address the question, how far are people within any of these frames as initial starting points, open to persuasion to shift frame?

The argument that underpins this analysis suggests that, while persuasion is possible, there are in fact some clear limits to the openness of consumers to persuasion to be interested in PETs other than those that their initial basic bias would direct them toward, just as the argument of the previous section showed that there are clear limits to the openness of businesses. For what really drives risk perception is situation. Bluntly, if we cannot change the real situation of consumers, then we should not expect their risk perception to shift greatly.

That said, there is a limited scope for frame shifting. So far, we have looked at the dominant influence of what we might call the *primary* situation — the long term, basic, underlying position in their society that a person occupies *vis-à-vis* large organisations, markets, the labour market, their peers, as modulated by specific institutional settings in particular contexts.

Some people may show very limited mobility, and for them, the survey methods on which some doubts were cast above, may have some limited validity if those surveys could distinguish the relevant people. Typically, those who remain within a single quadrant or frame across all the contexts of their lives are likely to be at the extremes of the matrix in Figure 7. For it is typically at the extremes where a single set of overarching features of the primary situation cast their shadow over every part of someone's life — for example, in acute poverty, great wealth, the engagement of one's whole life in a movement or community, or the dominance of a church or an all-consuming organisation of employment. Probably in most developed societies, it is a minority of the population whose lives are in these kinds of situations, and so we should expect significant proportions of people to show at least some mobility between contexts, typically between the more moderate positions.

By contrast, the most that we can expect by way of frame shifting persuasion from secondary situations (conversations or encounters in which information is offered that might run counter to the thought style engendered by the primary situation, modulated by the context) might be short-range moves between adjacent frames, which can only be sustained — if at all — as long as active persuasive pressure is sustained.

These arguments can be formalised by the following three hypotheses about the scope for persuasion to achieve these short-range moves:

- A. *Moves from one extreme to the other extreme of either diagonal frame face lower hurdles than do vertical and horizontal moves*

For example, one reason why some business and law enforcement interests can sometimes ally on privacy issues, is that there is an affinity between the extremes along the positive diagonal. Some business leaders, for example, take the view that “if you have nothing to hide, then you shouldn’t care about privacy”: it became clear in the study discussed above that this is a stance typically used to mark out oneself as a decent person and to challenge others to put themselves in the clear by agreeing: in short, it functions as a blame-deflection tool. The law enforcement agents who take the view that unknown but large numbers of people do indeed have something to hide and that is precisely why privacy should not be protected can therefore ally with those who work with the “nothing to hide” frame, for each is principally interested in sorting sheep from goats among potentially suspect populations. Conversely, the “conspiracy” frame of the privacy activists and their deterministic view of information technology as intrinsically oppressive has an affinity with the “indignity” frame’s view that large organisations necessarily exploit people: in effect, the affinity reflects the blame-mobilising role of these extreme frames.⁴⁵ These affinities make moves between these frames easier to make, in certain kinds of conversations, than certain other moves.

- B. *Moves along diagonals within quadrants face lower hurdles when they are moves outward than when they are moves inward toward the centre, where the primary situation makes for any vulnerability in the anchoring to the reference frame*

Where, for example, people are insecurely situated in the labour market, it is much easier for them to move from a “lack of control” frame about their privacy vis-à-vis employers and government bodies to an “indignity” frame, when they are put into the secondary situation of a conversation with others whose reference frame is that of indignity. Likewise, those who are insecurely situated in their community of residence and feel under surveillance can move more easily from an injustice to a conspiracy frame if they are in conversation with less moderately enclaved persons than themselves.

- C. *Vertical and horizontal moves between any of the moderate positions are easier than moves between the moderate form of any quadrant and the extreme form of another quadrant related horizontally or vertically (i.e. not diagonally, for a group for whom the baseline or reference frame is anchored reasonably securely as a moderate one.*

In the study discussed, there were some focus groups in which people came from relatively diverse primary situations. In conversation together, many of them were able to move relatively smoothly between, for example, “lack of control” and “injustice” frames, but in no case did we observe people moving from “indignity” to “inconvenience” frames. However, some of the income support claimants were able, after a lot of work together, occasionally to reach along the diagonal to speak from an “injustice” frame.

By what means can regulatory bodies either change primary situations or create secondary situations, in which consumers might be influenced to shift frames? Firstly, regulators have no monopoly upon risk communication in this area, nor do they have a captive audience: there are many commercial and other organisations offering alternative messages. Secondly, it should be noted that all the means of persuasion and propaganda available to governmental bodies are relatively blunt instruments. That is to say, there is no certainty at all that applying any particular tool that might lead to someone abandoning a certain way of thinking about privacy will necessarily lead to them taking up the particular other frame about privacy risk that the governmental body would prefer them to adopt. Once people are dislodged from one anchoring, their path is not predetermined.⁴⁶ The greatest change in influencing where people end up is to influence their primary situation, rather than only to offer information to influence the secondary situation.

Changing the basic primary situations of populations is the most ambitious goal of policy, and involves complex mixes of the uses of incentive, authoritative regulation, information and persuasion that go far beyond the scope of the present paper, for such things are in general undertaken for much larger and wider reasons than simply to influence preferences for privacy.⁴⁷ Changing secondary situations basically involves using informational tools — education, information provision, persuasion, *etc.*, whether through formal organisations such as schools or through informal systems such as the media. Research has generally found that the results of such strategies are highly variable and contingent upon the particular circumstances.⁴⁸ If they can be sustained over very long periods, with enormous commitment from all local institutions, on defined target groups, and delivered at such intensity that the information comes to have some of the power of an institution, then, public health research suggests, effects can be achieved, but this involves vast resources.⁴⁹ In these situations, in effect, the sustaining and embedding of the information campaign is beginning to impact upon the primary situation of local populations in the context of their health behaviour. For example, it is a now well established finding in media studies — for example, in studies on the impact of the deliberate attempt to make use of the media to “improve the public understanding of science” (which almost invariably means to attempt to attenuate public perception of some technological risk⁵⁰) — that messages from the media are not passively received but are considered by lay publics much more critically than many “experts” imagine, according to their local knowledge, prior worldviews and basic situation.⁵¹ When experts attempt risk communication and persuasion beginning from hierarchical or individualist assumptions, as they tend to do, and where segments of the public do not share those assumptions, because of their particular situation, they will not be persuaded and may simply not engage with the information offered.⁵² There are many examples where extensive public information campaigns have effected no significant change in the opinions of most people — indeed, this is the now well-established finding of political scientists studying general election campaigns which goes back to the 1940s⁵³ — election campaigns have no significant net effects and indeed often no very large individual-level effect, unless it is to polarise still further those who began with more extreme positions. In general, on those occasions when the media sustains attention beyond the usual “issue attention cycle” upon some major issue, they are thought to be more effective in focusing attention than in persuading — as the cliché has it — in telling people what to think about rather than what to think.⁵⁴ However, for issues such as privacy that do not tend to be focused upon by the media beyond the issue attention cycle, even this is not particularly promising. Social psychological work has found that even those persuaded to adopt a more positive attitude to something may still not actually buy it.⁵⁵ This would, presumably apply to a privacy-respecting service using PETs as much as to anything else. Even where messages can be sustained over time, despite the “issue attention cycle” of the media, “cultivation” effects in inducing people to change their preferences cannot be relied upon.⁵⁶ This psychological finding makes sense when understood as a symptom of the dominance of the primary situation on thought style in the manner set out above. Only when people are persuaded to shift their sense of their own identity — that is, in the terms used here, when a change can first be made in the primary situation — have psychologists observed significant attitude change effects, to adopting attitudes that they consider consonant with the identity being adopted.⁵⁷ Yet most public information campaigns are addressed at the level of the particular risk, or the particular context

— such as online shopping, or the medical setting, or banking — rather than at the larger level of the primary situation.

This is not to say that only in rare and very exceptional cases can public information campaigns work. Rather it is to suggest that they may not work in the ways intended, that they cannot necessarily overcome the effects of other forces, and they have to be designed with the greatest care, targeted very carefully rather than attempt blanket coverage, focus on very specific risks and offer very specific reasons to adopt quite specific solutions, be sustained over long periods, and work with the basic moral norms of the target segment of the public and engage their sense of identity and situation.⁵⁸

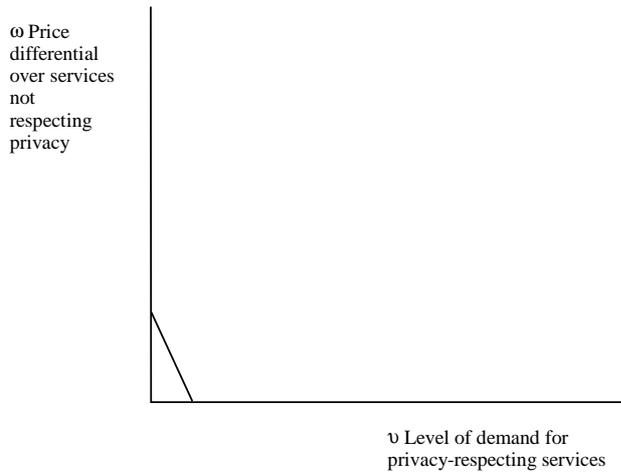
The issues of price sensitivity and transaction cost recognition can be dealt with more briefly. The more *individualistic* are most likely to be attuned to a basically proportionate and linear sensitivity to price increments. Among them, in a roughly proportionate manner, we should expect that as price differentials for privacy-enhanced services rise above prices for services that offer less respect for privacy, the less they will be willing to demand privacy-respecting services and the PETs embedded in them. Conventional economists' demand curves make most sense for this group. The more *enclaved* groups are likely to exhibit a kinked curve for price sensitivity, in the sense that they are more likely to be willing to pay higher prices for privacy protection, and as the cost of privacy rises above a certain threshold, unlike the individualists, they will not simply give up on it, but exercise voice rather than exit,⁵⁹ in order to demand regulation to reduce the cost of the more drastic privacy protections that they care about most. The more *hierarchical* will be price sensitive, but will show a kink at a higher point than the enclaved, for although regulation will be important to them, they will be more willing to accept that, within a defined band, it is reasonable for organisations to charge prices that reflect costs. Price sensitivity is likely to be lowest for the *isolates*, for they will see little benefit from technologies of these kinds in the context of their dealings with the organisations they face. Figure 9 summarises what we should expect using conventional simplified demand curves.⁶⁰ Again, it should be remembered that many people will exhibit a different curve in different contexts.

In order to understand how open to influence consumer demand for PETs might be, it remains to consider the sensitivity of consumers to the non-monetary transaction costs of search, mobility between providers, and their own time and effort in use. It is to be expected that individualists, again, will be proportionately sensitive, for to them, time is money in a straightforward way. By contrast, those willing to price their own time and effort at the lowest rate in order to secure the privacy protections they care most about are likely to be the more enclaved, while the more hierarchical will be willing to bear moderate time costs. The issue hardly arises for isolate/fatalists about privacy, for their interest is so low in any case. Therefore, the quasi-price sensitivity curves for the partly non-monetised transaction costs will look very similar to those for price differentials between privacy-respecting services using PETs and non-privacy-respecting services using none.

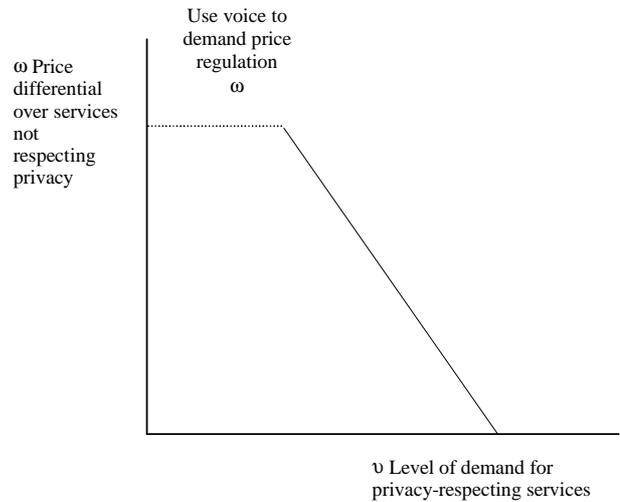
Bringing business and consumer interest together

It will not have escaped the reader that Figure 2, describing the basic situations of businesses, and Figure 7, describing the basic situations of consumers, at root use the same analysis. They are both applications of Figure 6 to their respective fields. The vertical dimension in Figure 2 that describes the extent of monopolistic or oligopolistic ordering of markets is essentially the same thing as the “constraint” dimension in Figure 7 upon consumers, for it captures the issue of the degree to which the market is ordered by something, that is by coercive or by competitive power (social regulation). Likewise, the dimension of surveillance by the wider community in Figure 2 that explains both willingness and opportunity to exploit, is essentially the same as the dimension of “bonds” for consumers, for it captures the extent of accountability to others (social integration). This is important, because it enables us to understand the dynamics of the relationship between businesses' ability and willingness to offer privacy-respecting services and consumers' ability and willingness to demand those services.

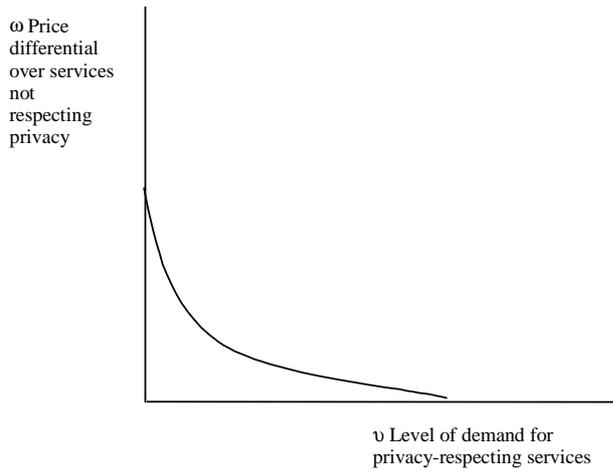
Figure 9. Demand curves for PETs for consumers in the four basic situations



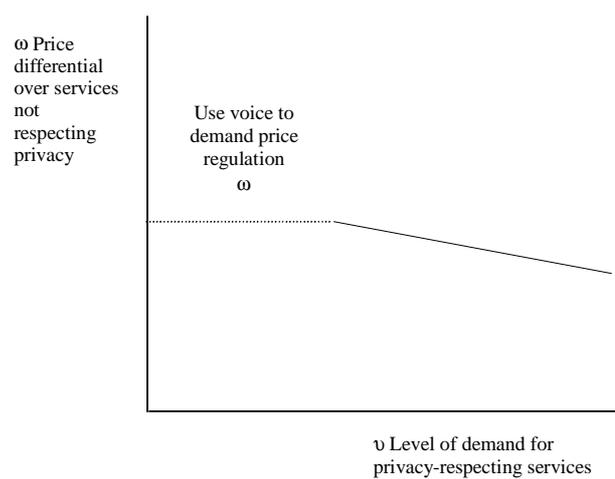
Isolate / fatalist consumer's curve for services using PETs



Hierarchical consumer's demand curve for services using PETs



Individualist consumer's curve for services using PETs



Enclaved consumer's demand curve for services using PETs

The institutional situation that shapes consumers' risk perceptions and hence their preferences about privacy will, of course, be shaped by aspects of people's lives that go far beyond their encounters with businesses. Those additional institutional factors are shaped by their encounters with peers, with governmental bodies, with the law, with family and a host of other relationships. Nevertheless, in many situations, it may be possible for the institutional processes governing businesses and consumers to create a *sorting* process which would lead consumers and businesses in corresponding quadrants to gravitate toward each other.

The main sorting processes in any market, which enable businesses and consumers with similar characteristics, institutional styles and constraints, and responsiveness to similar concerns, to find each other, are, quite simply:

- In competitive markets, consumers’ willingness and ability to bear the transaction costs of search and mobility until they find suppliers they can trust or that offer them the protections they seek.
- In non-competitive markets, the ability and willingness of regulatory action or the fear of regulatory action, as a substitute for consumer action in search and mobility.
- Business strategies, based on hope, to invest in marketing in order to signal to consumers with the relevant preferences and, at least at the margin, in using advertising and other frame-shifting means of persuasion to influence those preferences.

Sorting is never perfect, of course, because in competitive markets where, unavoidably, there are significant search and mobility costs, new incoming consumers lack the experience that older, exiting consumers possess, and so, even if their preferences are stably formed — which is often far from being the case — they take some time to find the sector that most suits their preferences.

How much sorting, then, can we expect, even in the case most favourable to sorting? It can be argued that a reasonable level of sorting can be expected, at most, in three of the matching quadrants. Businesses in the sector under the spotlight may be able to attract enough enclaved consumers with strong preferences and those consumers will be willing to bear the transaction costs of search and mobility from other suppliers so that they can find businesses willing to meet their preferences. Likewise, more entrepreneurial businesses may be able to secure the interest of more individualist consumers for the range of price/privacy ratios that their menu of services can offer. Again, the large bureaucratic world of the orderly sector could attract enough hierarchical consumers for each sector to be sustainable, even if there is volatility among individual firms in each. However, there is a sector of businesses for which and a segment of the consumer population for whom sorting is necessarily limited. By definition, the criminal sector will catch whoever it can, and not only isolate-fatalist consumers even if they are the most vulnerable; conversely, isolate-fatalist consumers may show up in any of the economic sectors of businesses and will, again by definition, be unlikely to see much point in bearing the costs of search and mobility to shift sector, even in this “sorting” scenario.

Suppose a reasonable level of three-quadrant sorting were achieved. Even then, it is important to note that there might still be some conflicts, for the match of PETs which businesses and consumers might want may not be exact. Figure 10 shows the extent of the match in a “sorting” scenario, by bringing together the key elements of Figures 5 and 8.

As we might expect, the area of least conflict is the hierarchical/orderly sector, (when adequately regulated), where consumers can most readily adjust to what cost pressures and situations lead businesses to be most open to offering. However, it is quite possible that individualist consumers might demand readier access to data correction requests and more consent than businesses in the entrepreneurial sector might find profitable in the time horizons they prefer to work in, and even more likely that the more extreme enclaved consumers will demand privacy protections that are more expensive than the small and medium sized niche market businesses of the sector under the spotlight will find profitable. This is in line with the expectation on wider theoretical grounds that this zone would, at least under many situations, exhibit great tendency for conflict and schism between suppliers and consumers.⁶¹

Figure 10. The extent of match and mismatch under a three quadrant “sorting process” scenario

<i>Constraints / Barriers to entry</i>				
		ω		
<p>Businesses: Criminal sector Not open to any, but actively resistant to sorting mechanisms</p>	<p>Consumers: Isolate - fatalism [ignore, because passively unresponsive to sorting mechanisms]</p>	<p>Businesses: Orderly sector most open: <i>alerting, information</i> somewhat open: <i>subject access, identification limitation, data change request</i></p>	<p>Consumers: Hierarchy most interested in: <i>alerting, information</i> somewhat interested in: <i>subject access, data change opportunity, ? identification limitation</i></p>	
<p>Businesses: Entrepreneurial sector most open: <i>alerting, information, subject access</i> somewhat open: <i>identification limitation, data change request</i></p>	<p>Consumers: Individualism most interested in: <i>subject access, data change opportunity</i>, somewhat interested in: <i>consent by opt-out, information</i></p>	<p>Businesses: Sector under the spotlight most open: <i>alerting, information, subject access, identification limitation, data change request</i> somewhat open: <i>consent, collection limitation, destination limitation</i></p>	<p>Consumers: Enclave most interested in: <i>consent by opt-in, collection type limitation, collection context limitation, identification limitation, destination limitation, notification</i> somewhat interested in: <i>subject access</i></p>	<p>υ <i>Bonds/ Community surveillance</i></p>

If, on the other hand, there are institutional blockages to sorting — for example, because there are insufficient numbers of enclaved consumers to sustain a highly responsive sector of businesses responding to those enhanced levels of preference for privacy, or if the costs of mobility for at least some groups of consumers to the sector that might otherwise best suit their preference profile are high — then we can expect even greater conflict. In situations of conflict, a number of outcomes are possible. One interesting outcome is the possibility that conflict itself represents a significant change to the primary situation of the consumer, which causes them to shift frame altogether. They may find that they adjust their frame to the sector they find themselves in which would produce a delayed or lagged sorting process. Alternatively, they may react against the institutions of that sector.⁶² There may be pressures in each direction. However, we should expect that in a market where there is limited competition and so the consumer can exercise few choices other than to use the service offered by the incumbent, the pressures would be more powerful to adapt their frame to that of the sector in which the monopolist is located. In the former case, we have an example of persuasion of consumer by business, and in the latter, the reverse. Just as was noted above about public information campaigns, it is not possible in advance to predict just what will be the destinations of people dislodged from their location in social organisation, whether deliberately by policy action or otherwise.

A key question for public policy, then, is whether it should be a goal of policy to remove institutional and market-based barriers to sorting of this kind. The implication of the present argument is that if we want to reduce conflicts, then — all other things being equal (such as the costs and risks of removing barriers, and the possibility of unintended consequences), this might well be worth doing.

Conclusion

The argument of this paper is that there is some scope for persuading businesses and consumers to be more interested respectively in offering and in demanding services supported by privacy-enhancing technologies, even if those services are slightly more expensive than services that do not protect privacy. However, it has been argued that this scope is circumscribed in ways that can and should be understood by governments and movements seeking to promote the use of privacy-enhancing technologies. There is scope to present certain kinds of PETs in ways that will make them more attractive to businesses in certain types of situation and to consumers in certain types of situation. If persuaders can work with the grain of the constraints, the institutional contexts, the basic assumptions and outlooks of businesses and consumers in these situations, and if they can develop rich appreciations of what may interest them, then they may be able to target communications about PETs to quite tightly defined constituencies in ways that will make a significant difference.

On the other hand, the argument here suggests that it would be a mistake to attempt persuasion on a one-size-fits-all basis, or to imagine that any business and any consumer can be persuaded to be interested in any kind of protection against any important privacy risk, still less at any cost. The paper argues for a certain modesty in the ambition of policy makers: the beginning of wisdom for persuaders is to accept that policy failure is the more likely the more ambitious are the goals for those to be persuaded and the range of things about which persuasion is to be attempted. Moreover, the most successful persuasion induces relatively short-range movement in how people think. Dramatic “road to Damascus” conversions are rare, and not usually amenable to being induced by deliberate policy action.

For would-be persuaders for PETs, then, the first task is to understand the ways in which businesses and consumers segment by situation. The second is to derive from this, an appreciation of which types of PETs they may be open to persuasion about. The third is to develop a clear understanding of the basic outlooks within which those PETs will have to make sense. The fourth is to identify the tools and instruments available to persuaders with which to address each of these constituencies.

The good news that is implied in the argument of this paper, is that some privacy protections matter to some degree to people in a very wide variety of situations. The bad news is that it will be a considerable labour for policy makers and persuaders to work out more exactly just what matters to just whom.

NOTES ON ANNEX II

1. Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, 1995, *Privacy enhancing technologies: the path to anonymity, vols I and II*. See also Registratiekamer for Netherlands, 1999, *Intelligent software agents: turning a privacy threat into a privacy protector*, Information and Privacy Commissioner for Ontario, Canada and Registratiekamer for Netherlands, Toronto and Rijkswijk. See also the typology offered in Burkert H, 1997, 'Privacy enhancing technologies: typology, critique, vision', in Agre PE and Rotenberg M, eds, 1997, *Technology and privacy: the new landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.
2. Cf. the general characterisation given in Burkert H, 1997, 'Privacy enhancing technologies: typology, critique, vision', in Agre PE and Rotenberg M, eds, 1997, *Technology and privacy: the new landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.
3. Indeed, many of the same debates will, no doubt, in due course, arise about them as arise in connection with safety devices: do they work, do they induce complacency and undermine vigilance, do they add to complexity in ways that may actually lead to privacy failures? For the major presentation of the argument that designing risk-reducing features into systems adds to complexity and can lead to failures, see Perrow C, 1999 [1984], *Normal accidents: living with high risk technologies*, 2nd edn, Princeton University Press, Princeton, New Jersey. For a recent statement of the argument that adding risk-reducing systems induces people to be complacent about risk, see Adams J, 1995, *Risk*, UCL Press, London. The principal statement of the argument that designing in risk-reducing features produces inflexible, rigid systems that often increase the likelihood of the very risks these features are meant to reduce, is Wildavsky A, 1988, *Searching for safety*, Transaction Publishers, New Brunswick, New Jersey. Indeed, Burkert's discussion raises the possibility that there may be privacy failures in systems using these technologies for each of these reasons, although Burkert does not draw the analogy with the wider risk management literature: Burkert H, 1997, 'Privacy enhancing technologies: typology, critique, vision', in Agre PE and Rotenberg M, eds, 1997, *Technology and privacy: the new landscape*, Massachusetts Institute of Technology press, Cambridge, Massachusetts, 125-142.
4. Federal Trade Commission, 2000, *Privacy online: fair information practices in the electronic marketplace: a Federal Trade Commission report to Congress*, May, Federal Trade Commission, Washington DC, available at <http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf>. See also Consumers International, 2001, *Privacy@net: an international comparative study of consumer privacy on the internet*, Consumers International, London, available at <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf>.
5. This research is being conducted in the department of management and information technology at Bentley College, Massachusetts: Mary Culnan, personal communication, 3rd October 2001.
6. Jowett GS and O'Donnell V, 1999, *Propaganda and persuasion*, 3rd edn, Sage, London, 171.
7. Allison GT, 1971, *Essence of decision: explaining the Cuban missile crisis*, Little, Brown, Boston: see Allison GT and Zelikow P, 1999, *Essence of decision: explaining the Cuban missile crisis*, 2nd edn, Addison Wesley Longman, New York, 307. The original formulation of this maxim is attributed to Rufus Miles, a US federal administrator in the 1960s who managed a number of "Great Society" programme agencies under President Johnson, and worked both in the Executive Office of the President and in the Bureau of the Budget, and has been called "Miles' Law": see Stillman R, 1999, "Where you stand depends on where you sit" (or, yes, Miles' also applies to public administration basic texts), *American review of public administration*, 29, 1, 92-97.
8. Douglas M, 1986, *How institutions think*, Routledge and Kegan Paul, London; Thompson M and Wildavsky A, 1986, 'A cultural theory of information bias in organisations', *Journal of management studies*, 23, 3, 273-286.

9. For a discussion of the economics of inducing businesses to internalise costs that they could externalise and might fear others will externalise, see Baumol WJ, with Blackman SAB, 1991, *Perfect markets and easy virtue: business ethics and the invisible hand*, Blackwell, Oxford, *passim* but esp. ch.3. Some people would say that this is a problem of getting businesses to internalise the costs of providing public goods. I avoid putting the problem in this way for two reasons. First, there is a debate about just how far privacy protection is a public good, and how far the divisible character of the management of personal information makes it a private good: see *e.g.* Spinello RA, 1998, 'Privacy rights in the information economy: review of Legislating privacy: technology, social values and public policy, Priscilla Regan, Chapel Hill: UNC Press, 1995', *Business ethics quarterly*, 8, 4, 723-742. I have no wish to enter that arcane question here. Secondly, the question of what counts as a public or a private good also depends "on where you sit": see Wildavsky A, in Wildavsky A, ed. by Chai S-K and Swedlow B, 1998, 'At once ubiquitous and elusive, the concept of externalities is either vacuous or misapplied', in Wildavsky A, 1998, *Culture and social theory*, Transaction Publishers, New Brunswick, New Jersey, 55-84. In any case, the argument can be stated without the assumptions involved here, and the usefulness of analogy between PETs and environment-protecting technologies or business ethics does not depend on making these assumptions about externalities and public goods.

10. One might assume, for the present purpose, that it can be solved by administrative means, such as managerial directive or by internal regulation within government. In practice this is not straightforward, as two generations of implementation research have shown. However, the experiment within the British National Health Service since the report of the Caldicott Committee will provide an invaluable case study against which to test the rival claims about the efficacy of administrative direction as a strategy for securing compliance with privacy compliance in the public sector: see Department of Health, 1997, *The Caldicott Committee report on the review of patient-identifiable information*, Department of Health, London: and see also the subsequent guidance and reports on implementation available at www.doh.gov.uk/nhsexipu/confiden/. It is too early as yet to evaluate the lessons from this experience. In practice, many of the considerations that apply to the account of the openness of businesses to persuasion also apply to government agencies, but with some complex differences that cannot be explored here. For an overview of the constraints and incentives for frontline staff not to internalise costs that the centre might like them to, see Lipsky M, 1980, *Street level bureaucracy: dilemmas of the individual in public services*, Russell Sage Foundation, New York. On the general issues of implementation challenges of using managerial direction to induce subaltern agencies to internalise costs, see Bardach E, 1977, *The implementation game*, Massachusetts Institute of Technology Press, Cambridge, Massachusetts. Those interested in the difficulties of using internal regulation should consult, *e.g.* Hood C, Scott C, James O, Jones G and Travers T, 1999, *Regulation inside government: waste-watchers, quality police and sleaze-busters*, Oxford University Press, Oxford. At least in theory, if public sector agencies were to offer services that provided better respect for privacy and made greater use of PETs, this might raise consumers' expectations and increase their familiarity with the technologies, which might have spillover effects into their behaviour vis-à-vis the commercial bodies with which they deal, and through public purchasing of services from the private sector, there might be supply-side influences too. However, the history of, for example, equal opportunities practices in the public sector suggests that we might want to be cautious about the speed and the strength of these spillover effects, and their robustness to shocks and their power to overcome the resistance of countervailing commercial and institutional pressures.

11. Arthur B, 1990, 'Positive feedbacks in the economy', *Scientific American*, Feb, 92-99; Rosenberg N, 1994, *Exploring the black box: technology, economics and history*, Cambridge University Press, Cambridge; David PA, 1985, 'Clio and the economics of QWERTY', *Economic history*, 75, 2, 332-337; Pool R, 1997, *Beyond engineering: how society shapes technology*, Oxford University Press, New York, ch.5.

12. On the information asymmetry between regulators and the regulated in favour of the latter, see Klein RE and Day P, 1987, 'The regulation of nursing homes', *Milbank quarterly*, 65, 3, 303-347.

13. For a discussion of sense-making, which shows that it is not simply a reflection of instrumental economic calculation, see Weick KE, 1995, *Sensemaking in organisations*, Sage, London and Weick KE, 2001, *Making sense of the organisation*, Blackwell, Oxford.

14. On the high transaction costs of time and effort that have limited willingness to engage, for example, in home composting, see Åberg H, Dahlman S, Shanahan H, and Säljö R, 1996, 'Towards sound environmental behaviour: exploring household participation in waste management', *Journal of consumer policy*, 19, 1, 45-67.
15. Bech-Larsen T, 1996, 'Danish consumer's attitudes to functional and environmental characteristics of food packaging', *Journal of consumer policy*, 19, 3, 339-363; Thøgersen J, 1999, 'The ethical consumer: moral norms and packaging choice', *Journal of consumer policy*, 22, 4, 439-460; Thøgersen J, 1994, 'Monetary incentives and environmental concern: effects of a differentiated garbage fee', *Journal of consumer policy*, 17, 4, 407-442.
16. Friedman M, 1996, 'A positive approach to organised consumer action: the "boycott" as an alternative to the boycott', *Journal of consumer policy*, 19, 4, 439-451.
17. Neuner M, 2000, 'Collective prototyping: a consumer policy strategy to encourage ecological marketing', *Journal of consumer policy*, 23, 2, 153-175 at 172.
18. Sethi SP and Sama LM, 1998, 'Ethical behaviour as a strategic choice by larger corporations: the interactive effect of marketplace competition, industry structure and firm resources', *Business ethics quarterly*, 8, 1, 85-104.
19. I have made one change of a substantive nature to the Sethi and Sama analysis. I have renamed and amended the analysis of the sector described by the quadrant with low willingness to exploit but many opportunities to exploit. Although I have followed them in deriving from the characteristics of its location, the importance here of consumer pressure, reputation and good will, I have dropped their stress on certain other factors. In Sethi and Sama's account, this is described as the "high growth" sector, associated with what they call the middle stage of the technological and product cycle, before innovative products have yet reached mass markets. However, these features seem to be highly contingent: in many niche markets which the basic structural position on these dimensions describes, indeed, high growth and readiness for mass markets do not seem to be observed. I have tried to focus on those features that follow logically or causally from the structural position on the two dimensions.
20. For an institutionalist account of the dynamics of markets which explains the production of preferences as well as the structure of opportunities in the same process, see Douglas M, 1986, *How institutions think*, Routledge and Kegan Paul, London; Powell WW and DiMaggio PJ, eds, 1991, *The new institutionalism in organisational analysis*, University of Chicago Press, Chicago; Thompson M, Ellis R and Wildavsky A, 1990, *Cultural theory*, Westview Press, Boulder, Colorado; see also Wildavsky A, 1994, 'Why self-interest means less outside of a social context: cultural contributions to a theory of rational choices', *Journal of theoretical politics*, 6, 2, 131-159, repr. in Wildavsky A, 1998, *Culture and social theory*, ed Chai S-K and Swedlow B, Transaction Publishers, New Brunswick, New Jersey, 231-258. esp. at 251ff.
21. The recent OECD study offers what is, in the terms used here, a technological classification (at para 2) and a functional classification (at para 12). Closest to the present risk type approach is what the OECD study calls "policy effect" (at para 12): Working Party on Information Security and Privacy, 2001, *Annex 2: A study of privacy-enhancing technologies*, Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development, Paris.
22. Ouchi WG, 1980, 'Market, bureaucracies and clans', *Administrative sciences quarterly*, 25, 2, 120-142.
23. CEN, the European Standards Institute, put out a first version of a consultation paper on precisely this. However, the revised version recommended that management standards should not, after all, be initiated but that developments in the International Standards Organisations and other bodies should be monitored, and that the only work to be taken forward should be on contract terms and on criteria for Web-based privacy seals, and to produce a further report on PETs: see *Comité Européen de Normalisation (CEN: European Committee for Standardisation)*, 2001, 'Initiative on privacy standardisation in Europe (IPSE): Discussion draft - report by Project Team for the second CEN Information Society Standardization System (ISSS) Data Privacy Open Workshop, Paris 27th September 2001', CEN, Brussels, available at <http://www.cenorm.be/issc>.

24. See e.g. Gomulka S, 1990, *The theory of technological change and economic growth*, Routledge, London, ch. 6, esp. 93.
25. 6 P, 1998 with Lasky K and Fletcher A, 1998, *The future of privacy, vol. II: public trust in the use of private information*, Demos, London.
26. Equifax 1995, *The Harris-Equifax mid-decade consumer privacy survey*, Equifax, Atlanta, Georgia; Henley Centre for Forecasting, 1995, *Dataculture: privacy, participation, and the need for transparency in the information age*, Henley Centre for Forecasting, London; Direct Marketing Association and Informix, 1997, *The new information trade*, Direct Marketing Association and Informix, London.
27. C.f. Sniderman P, 1993, 'The new look in public opinion research', in Finifter AW, ed, 1993, *Political science: the state of the discipline II*, American Political Science Association, Washington DC, 219-245 at 233.
28. The psychometric tradition has been a fertile source of observation of the distribution of types of bias in risk perceptions — in short, it has been helpful in describing the dependent variable. For overviews, see Slovic P, 1992, 'Perception of risk: reflections on the psychometric paradigm', in Krimsky S and Golding D, eds, 1992, *Social theories of risk*, Praeger, Westport, Connecticut, 117-152; Slovic P, 2000, *The perception of risk*, Earthscan, London; Kahneman D, Slovic P and Tversky A, eds, 1982, *Judgment under uncertainty: heuristics and biases*, Cambridge University Press, Cambridge; Kahneman D and Tversky A, 2000, *Choices, values and frames*, Cambridge University Press, Cambridge. This approach has been developed in the recent work on "mental maps": see Morgan G, Fischhoff B, Bostrom A and Atman CJ, 2001 forthcoming, *Risk communication: a mental models approach*, Cambridge University Press, Cambridge; Bostrom A, Fischhoff B and Morgan GM, 1992, 'Characterising mental processes of hazardous processes: a methodology and an application to radon', *Journal of social issues*, 48, 4, 85-100, repr. in Löfstedt R and Frewer L, eds, 1998, *The Earthscan reader in risk and modern society*, Earthscan, London, 225-238; Jungermann H, Schütz H and Thüning M, 1988, 'Mental models in risk assessment: informing people about drugs', *Risk analysis*, 8, 1, 147-155, repr. in Löfstedt R and Frewer L, eds, 1998, *The Earthscan reader in risk and modern society*, Earthscan, London, 213-224. For slightly different approach, see Renn O, 'Three decades of risk research: accomplishments and new challenges', *Journal of risk research*, 1,1, 49-71.
29. For a critique of these and other weaknesses, see Douglas M, 1985, *Risk acceptability according to the social sciences*, Russell Sage Foundation, New York and Routledge and Kegan Paul, London.
30. This is an argument that is hardly controversial in anthropology and sociology, where since Durkheim and Evans-Pritchard, the sociology of knowledge has developed this argument.
31. Contrary to the post-modernists who hold that there is indefinite variation, entirely unanchored in the realities of social life.
32. Durkheim É, 1951 [1897], *Suicide: a study in sociology*, tr. Spaulding JA and Simpson G, Routledge, London.
33. Douglas M, 1970, *Natural symbols: explorations in cosmology*, Routledge, London; Douglas M, 1982 [1978], 'Cultural bias', in Douglas M, 1982, *In the active voice*, Routledge and Kegan Paul, London, 183-254. For the application to the perception of risk, see Douglas M, 1992, *Risk and blame: essays in cultural theory*, Routledge, London; Douglas M and Wildavsky A, 1982, *Risk and culture: an essay on the selection of technological and environmental dangers*, University of California Press, Berkeley; Adams J, 1995, *Risk*, UCL Press, London; Thompson M, Ellis RJ, and Wildavsky A, 1990, *Cultural theory*, Westview Press, Boulder; Coyle DJ and Ellis RJ, eds, 1993, *Politics, policy and culture*, Westview press, Boulder, Colorado; Dake K and Wildavsky A, 1993, 'Theories of risk perception: who fears what and why?', in Burger EJ, jnr, ed, 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Douglas M, 1990, 'Risk as a forensic resource', *Daedalus*, 119, 4, 1-16; Douglas M, 1997, 'The depoliticisation of risk', in Ellis RJ and Thompson M, eds, 1997, *Culture matters: essays in honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 121-132; Ellis RJ and Thompson F, 1997, 'Seeing green: cultural biases and environmental preferences', in Ellis RJ and Thompson M, eds, 1997, *Culture matters: essays in*

- honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 169-190; Gross JL and Rayner S, 1985, *Measuring culture: a paradigm for the analysis of social organisation*, Columbia University Press, New York; Thompson M, Grendstad G and Selle P, eds, 1999, *Cultural theory as political science*, Routledge, London; Rayner S, 1992, 'Cultural theory and risk analysis', in Krinsky S and Golding D, eds, 1992, *Social theories of risk*, Praeger, Westport, Connecticut, 83-116.
34. Ouchi WG, 1980, 'Market, bureaucracies and clans', *Administrative sciences quarterly*, 25, 2, 120-142. For a collection of papers on the three fold conception, see Thompson G, Frances J, Levačić R, and Mitchell J, eds, 1991, *Markets, hierarchies and networks*, Sage, London. The major early theoretical statements in economics on markets and hierarchies are contained in Coase RH, 1937, 'The nature of the firm', *Econometrica*, 4, 386-405. A more recent major statement in Williamson OE, 1986, *The economic institutions of capitalism*, Free Press, New York. See also Pitelis C, 1991, *Market and non-market hierarchies: theory of institutional failure*, Blackwell, Oxford, and Miller GJ, 1992, *Managerial dilemmas: the political economy of hierarchy*, Cambridge University Press, Cambridge.
35. In sociometric analysis of social networks, there are well developed structural measures of isolation: see e.g. Wasserman S and Faust K, 1994, *Social network analysis: methods and applications*, Cambridge University Press, Cambridge; there are also many qualitative studies examining the outcomes associated with isolate positions, especially in studies on adolescence: see e.g. Cotterell J, 1996, *Social networks and social influences in adolescence*, Routledge, London. The "social capital" literature has in effect contrasted outcomes associated with isolate forms with outcomes associated with all other forms: see Putnam RD, 2000, *Bowling alone: the collapse and revival of American community*, Simon and Schuster, New York; Lin N, 2001, *Social capital: a theory of social structure and action*, Cambridge University Press, Cambridge. The sociological and social network analytical traditions also contain plenty of studies of enclaves — e.g. Elias N with Scotson JL, 1994 [1977], *The established and the outsiders: a sociological enquiry into community problems*, Sage, London — and of individualism — most famously Granovetter 1994 [1974], *Getting a job: a study of contacts and careers*, 2nd edn, University of Chicago Press, Chicago, and Burt RS, 1992, *Structural holes: the social structure of competition*, Harvard University Press, Cambridge, Massachusetts. For an overview, see 6 P, 2001, 'The governance of friends and acquaintances? Public policy and social networks', paper presented at the Economic and Social Research Council and Institute for Public Policy Research joint seminar, "Public policy and social networks: promoting social inclusion", 15 March, London. A classical study of the fatalistic outlook on risk associated with comparatively isolate forms is Banfield EC with Banfield LF, 1958, *The moral basis of a backward society*, Free Press, New York.
36. See 6 P, 2001, *Strategies for reassurance: public concerns about privacy and data sharing in government*, Performance and Innovation Unit, Cabinet Office, London.
37. Gamson WA, 1992, *Talking politics*, Cambridge University Press, Cambridge; for a discussion of the concept of a frame, see 6 P, 2001, 'What's in frame? Social organisation, risk perception and the sociology of knowledge', unpublished typescript, King's College, London.
38. For a critique of the argument that "balance" can be made as determinate a criterion for policy making as this bureaucratic hierarchical way imagines, see Raab CD, 1999, 'From balancing to steering: new directions for data protection', in Bennett CJ, and Grant R, eds, 1999, *Visions of privacy: policy choices for the digital age*, University Toronto Press, Toronto, 68-93.
39. 6 P, 2001, *Strategies for reassurance: public concerns about privacy and data sharing in government*, Performance and Innovation Unit, Cabinet Office, London. For an earlier version that situates many of the leading writers and thinkers about privacy within this two dimensional space, see 6 P, 1998, *The future of privacy, vol I: private life and public policy*, Demos, London, ch.4.
40. On the case for the "mobility" hypothesis, see Rayner S, 1992, 'Cultural theory and risk analysis', in Krinsky S and Golding D, eds, 1992, *Social theories of risk*, Praeger, Westport, Connecticut, 83-116.
41. See e.g. Grendstad G and Selle P, 1997, 'Cultural theory, postmaterialism and environmental attitudes', in Ellis RJ and Thompson M, eds, 1997, *Culture matters: essays in honour of Aaron Wildavsky*, Westview Press, Boulder, Colorado, 151-168; Dake K and Wildavsky A, 1993, 'Theories of risk perception: who

- fears what and why?', in Burger EJ, jnr, ed, 1993, *Risk*, University of Michigan Press, Ann Arbor, Michigan; Grendstad G, 2001, 'Nordic cultural baselines: accounting for domestic convergence and foreign policy divergence', *Journal of comparative policy analysis, research and practice*, 3, 5-29.
42. See Gross JL and Rayner S, 1985, *Measuring culture: a paradigm for the analysis of social organisation*, Columbia University Press, New York.
43. See e.g. Davies S, 1996, *Big brother: Britain's web of surveillance and the new technological order*, Pan, London.
44. Sniderman PM, Piazza T, Tetlock PE and Feld PJ, 1991, 'The American dilemma: the role of law as a persuasive symbol', in Sniderman PM, Brody RA and Tetlock PE, eds, *Reasoning and choice*, Cambridge University Press, New York.
45. On the central importance of understanding risk perception as essentially about the organisation of what to do with social processes of blame, see Douglas M, 1992, *Risk and blame: essays in cultural theory*, Routledge, London.
46. Thompson M, 1992, 'The dynamics of cultural theory and their implications for the enterprise culture', in Hargreaves Heap S and Ross A, eds, 1992, *Understanding the enterprise culture: themes in the work of Mary Douglas*, Edinburgh University Press, Edinburgh, 182-202.
47. For discussion of the tools of government, see Hood C, 1983, *The tools of government*, MacMillan, Basingstoke; Salamon LM with Lund MS, 1989, *Beyond privatisation: the tools of government action*, Urban Institute Press, Washington DC; Bemelmans-Videc M-L, Rist RC and Vedung E, eds, 1998, *Carrots, sticks and sermons: policy instruments and their evaluation*, Transaction Publishers, New Brunswick, New Jersey; Peters BG and van Nispen FKM, eds, 1998, *Public policy instruments: evaluating the tools of public administration*, Edward Elgar, Cheltenham; 6 P, Leat D, Seltzer K and Stoker G, 1999, *Governing in the round: strategies for holistic government*, Demos, London.
48. Linder SH and Peters BG, 1998, 'The study of policy instruments: four schools of thought', in Peters BG and van Nispen FKM, eds, 1998, *Public policy instruments: evaluating the tools of public administration*, Edward Elgar, Cheltenham, 33-45.
49. See e.g. Maccoby N *et al*, 1977, 'Reducing the risks of cardiovascular disease: effects of a community based campaign on knowledge and behaviour', *Journal of community health*, 3, 1, 100-114.
50. Although practitioners in that field are not agreed on whether to admit that this is the case! See: Dierkes M and von Grote C, eds, 2000, *Between understanding and trust: the public, science and technology*, Harwood Academic Publishers, Amsterdam.
51. Irwin A and Wynne B, eds, 1996, *Misunderstanding science: the public reconstruction of science and technology*, Cambridge University Press, Cambridge; Irwin A, 1995, *Citizen science: a study of people, expertise and sustainable development*, Routledge, London; Bush J, Moffat S and Dunn CF, 2001, 'Keeping the public informed? Public negotiation of air quality information', *Public understanding of science*, 10, 2, 213-229.
52. Schwarz M and Thompson M, 1990, *Divided we stand: redefining politics, technology and social choice*, University of Pennsylvania Press, Philadelphia; Robins R, 2001, 'Overburdening risk: policy frameworks and the public debate about gene technology', *Public understanding of science*, 10, 1, 19-36.
53. The original finding was by Lazarsfeld PF, Berelson B and Gaudet H, 1948, *The people's choice: how the voter makes up his mind in presidential campaigns*, Columbia University Press, New York.
54. O'Guinn TC and Faber RJ, 1991, 'Mass communication and consumer behaviour', in Robertson TS and Kassarian HH, eds, 1991, *Handbook of consumer behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, 349-400 at 363. One recent British study claimed to find a much greater effect of newspaper biases on readers, at least some major issues, but the data are in fact consistent with the possibility of much greater reader selection than newspaper influence: Lacey C and Longman D, 1997, *The press as public educator: cultures of understanding, cultures of ignorance*, University of Luton Press, Luton.

55. Zimbardo PG and Leippe MR, 1991, *The psychology of attitude change and social influence*, McGraw Hill, New York.
56. O'Guinn TC and Faber RJ, 1991, 'Mass communication and consumer behaviour', in Robertson TS and Kassirjian HH, eds, 1991, *Handbook of consumer behaviour*, Prentice-Hall, Englewood Cliffs, New Jersey, 349-400.
57. Valins D, 1966, 'Cognitive effects of false heart-attack feedback', *Journal of personality and social psychology*, 4, 4, 400-408.
58. Weiss JA and Tschirhart M, 1994, 'Public information campaigns as policy instruments', *Journal of policy analysis and management*, 13, 1, 82-119.
59. Hirschman AO, 1970, *Exit, voice and loyalty: responses to decline in firms, organisations and states*, Harvard University Press, Cambridge, Massachusetts; Dowding K, John P, Mergoupis T and van Vugt M, 2000, 'Exit, voice and loyalty: analytic and empirical developments', *European journal of political research*, 37, 469-495.
60. For an example of representing the impact of the four basic styles upon economic representations of demand, see Wildavsky A with Fogerty D and Jeanrenaud C, 1998, 'The concept of externalities is either vacuous or misapplied', in Wildavsky A, 198, *Culture and social theory*, ed Chai S-K and Swedlow B, Transaction Publishers, New Brunswick, New Jersey, 55-84.
61. For the larger theoretical argument about schism and conflict in this sector, see Thompson M, Ellis RJ and Wildavsky A, 1990, *Cultural theory*, Westview Press, Boulder, Colorado.
62. For an account of the range of possible outcomes here, consider the paths traced in the "theory of surprise" in Thompson M, Ellis RJ and Wildavsky A, 1990, *Cultural theory*, Westview Press, Boulder, Colorado, ch. 5.