



Consumers International

Privacy@net

An international comparative study
of consumer privacy on the internet



Privacy@net

An international comparative study of
consumer privacy on the internet



Consumers International

Office for Developed and Transition Economies

Acknowledgements

This report was produced by Consumers International's Programme for Developed Economies and Economies in Transition, with financial support from the European Commission Directorate General XXIV (Consumer Policy and Consumer Health Protection).

Consumers International would also like to thank its member organisations that took part in the project (listed in full on page 42) and to extend a special thanks to David Banisar, Privacy International.

Written and researched by Kate Scribbins.

Coordinated by Naja Felter, Consumers International.

Assisted by Jo Mills, Consumers International.

Edited by Alina Tugend.

Designed and produced by Steve Paveley.

© January 2001

ISBN 19023 91 31 68

Contents

Introduction	5
Research findings: overall verdict	6
Policy recommendations	8
Collection of personal information	8
Use and disclosure of personal information	8
Access	9
Security	9
Oversight and Compliance	9
Redress	9
Privacy policies	9
Consumer action	10
Children	10
Background	11
Why this study?	11
What is privacy?	12
Privacy, data protection and electronic commerce	12
Internet security and privacy	13
Spam	13
Privacy laws	14
Europe and the United States	15
Children and internet privacy	15
The research	17
The project team	17
List of participants	17
Methodology	17
How sites were selected	18
What our assessment covered	19
What happens when consumers really shop using the internet?	20
Results	20

Results in detail	22
Site tried to place cookie on the computer	22
Certification schemes	25
Content of privacy policy	26
Information	26
Choice	26
Access	27
Security	27
Other aspects:	27
Appendix 1: Cookies	28
Appendix 2: Privacy laws	30
Sectoral Laws	31
Self Regulation	31
Appendix 3: Technologies of privacy	33
Limits of technology	33
Appendix 4: The questionnaire	35
1 Personal information collected by the site	35
2 Information about the privacy policy	37
3 The privacy policy	38
4 Cookies	38
5 Security of payment information	39
6 Conclusion	39
Appendix 5: The participants	40
Appendix 6: Five steps to protecting your privacy online	42
Footnotes	43

Introduction

The growth of the internet and electronic commerce has created threats to consumers' privacy on an unprecedented scale. Intimate details about a user's private life are now an open book for those who wish to track down such information, yet consumers often do not know that every time they use the internet, they leave behind a detailed trail of personal information.

For example, few consumers are aware that companies use comprehensive databases to build up a profile of customers in order to target advertising. Some companies use the information to set pricing, selectively raising prices for some customers. Financial and personal information is stolen every day and used fraudulently to purchase goods and get credit.

Even more worrisome is that many sensitive documents, such as financial and medical records that were previously stored in separate databases, can now be placed online, frequently without consumer consent or adequate privacy protection.

Consumers International's research reveals that internet sites selling products and services to consumers in the United States and Europe fall woefully short of international standards on data protection. Most sites collect personal information but fail to tell consumers how that data will be used, how security is maintained, and what rights consumers have over their own information.

Despite tight European Union (EU) legislation, sites within the EU are no better at providing decent information to their customers than sites based in the US. Indeed some of the best privacy policies are to be found on US sites.

Concerns over confidentiality and security rank highly amongst reasons why consumers are reluctant to buy goods and services online. Unless policy makers and companies address issues of data protection, these concerns will continue to be well-justified, and electronic commerce may suffer as a result.

The objective of this research project was to find out how much information is collected from consumers when using the internet – whether for browsing, personal research or shopping – and to see how many sites take steps to protect the privacy of this information. By assessing more than 750 sites, Consumers International aimed to establish whether there was a significant difference in approach among internet sites based in the European Union and the United States.

This report starts by providing some general background to the issues surrounding electronic commerce and privacy. An overall verdict and key findings based on the results of the site assessment are then given on page 6, followed by the policy recommendations arising from these findings. Starting on page 17 the research method is described in detail. The in-depth results of the website assessments start on page 22.

Research findings: overall verdict

Despite the fact that the majority of the sites collected personal information from the user, only a tiny minority provided a privacy policy that gave users meaningful information about how that data would be used. Sites both in the US and EU fall woefully short of the standards set by international guidelines on data protection. The majority of sites ignore even the most basic principles of fair information use, such as telling consumers how their data will be used; how it can be accessed; what choices the consumer has about its use; and how security of that data is maintained. This widespread neglect of good privacy practice is made all the more worrying in the electronic commerce medium, where technologies for collection and use of data are developing so rapidly.

Despite tight EU legislation in this area, researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the US. Indeed, US-based sites tended to set the standard for decent privacy policies.

As US consumers do not have legal protection in this area, companies have to make more effort to reassure their users that their privacy will be protected. EU consumers are not only protected by legislation, but also have a data protection commissioner in each country looking out for their rights, and have a right to redress if the law is breached. However, in practice, EU sites do no better than US ones at keeping their users informed. Indeed it appears that many EU sites are failing to comply with EU rules that state that the consumer must be given the right to opt

out if their data is to be used for direct marketing purposes.

Key findings

The following section provides a summary of the most important findings of the website assessment. A fuller account of these findings and the underlying data is given in pages 22 to 27.

- Just over two thirds of the sites assessed (67%) collected some sort of personal information about the visitor during the process of using the site.
- Almost all sites that collected information asked for details that made it easy to identify and contact that person. Name, email name, postal address information and phone number were the most common type of information requested. The exception to this was news and information-type sites that tended to just ask visitors where they live in order to provide local news or weather.
- Most sites let the visitor visit and browse without overtly collecting information from them, but most encourage users to give information in order to use the site fully, for example by “personalising” the site, or signing up for membership. This enables the user to receive information that may be relevant to his or her life (for example local news and weather or a newsletter), but also provides an opportunity for the site to collect plenty of data about the consumer.
- Fifty-eight percent of the sites that collected

information had a privacy policy. Of sites that collected personal information from their users, *health* sites were the least likely to have a privacy policy. *Most popular* sites within the US were the most likely to have a privacy policy. *Most popular* sites based in the EU, and US-based *financial* sites, also performed well. (see page 18 for definitions of site categories).

- Privacy policies, however, were not always easily accessible. Only a third (32.5%) of sites that collected information and had a privacy policy alerted visitors to that privacy policy at the point where the information was collected. US-based *most popular* sites performed best, with 62.5% signposting their privacy policy at the point where information was collected. Sites should also signpost their privacy policies from their home page. Researchers found that just over a third of sites (39%) signposted their privacy policy from their home page. US-based sites were much more likely to do this than EU-based ones. 97.5% of US-based *most popular* sites signposted privacy policies from their home page.
- The vast majority of sites gave customers no choice about being on the site's own mailing list, having the customer's name passed on to affiliates, or to third parties. US *most popular* sites were most likely to give users a choice, despite the existence of legislation that obliges EU-based sites to provide consumers with a choice.
- Having a document called a privacy policy doesn't count for much unless it provides adequate information for the consumer. Very few of the privacy policies Consumers International assessed contained more than the bare minimum of information, and only a minority gave important information about the control consumers can have over their own data.
- However comprehensive a privacy policy is, it is worthless if the company fails to abide by it. Consumers International has found that some companies do breach their own policies. Therefore effective enforcement and a right to redress for consumers are vital.

Policy recommendations

Over the past three decades, countries have established a set of principles for data protection. These are commonly known as “fair information principles”, or FIPS. The US Department of Health, Education and Welfare first proposed the principles in 1974 and they were adopted into law in numerous countries. In 1981, the Organisation for Economic Cooperation and Development released extended guidelines based on the FIPS¹ and the Council of Europe incorporated them into a treaty for the processing of personal information in computerised systems that have been widely adopted in Europe.² Despite the widespread acceptance of these practices, Consumers International’s research shows that the majority of sites ignore even the most basic principles of fair information use, such as: giving consumers control over the collection and use of their information; giving them a right to access and correct that information; and ensuring security of their data.

Because so many companies ignore basic fair information principles, policy makers at the national and international level need to take urgent action to ensure that consumers are adequately protected. The following principles need to be incorporated into companies’ internal practices and national governments’ enforceable laws:

Collection of personal information

Information should only be collected if it is essential to the transaction. Any collection of non-essential information should be optional and clearly marked as such.

Sensitive information (as defined in international agreements such as the COE Convention 108 and the EU Data Protection Directive) should not be collected about the consumer except in very limited circumstances.

Information must be obtained directly from the consumer unless the consumer gives his or her prior consent allowing the information to be collected from another source.

The organisation should state the reason for collecting the information it has requested.

Information should be collected by fair and lawful means. Sites should never collect personal data in a non-transparent manner – for example by using hidden mechanisms such as web-bugs and cookies – without obtaining the consent of the consumer first. Whenever surveys, competitions or other forms of interaction are used to collect data, the organisation must make it clear to consumers that the information is being collected and how it will be used.

Use and disclosure of personal information

Personal information should be used only for the purpose for which it was collected, unless the consumer has given prior consent, as required by law.

Personal information should be kept only as long as necessary to fulfil that purpose.

Sensitive personal information should not be used or disclosed without the prior consent of the user.

If the organisation offers any options regarding using or disclosing personal information – such as passing it on to another company – the information should be available online and the consumer should be able to respond online. The user should not be told to write to a separate address in order to limit the use of his or her data.

If an organisation dissolves, files for bankruptcy, is acquired by another organisation, or otherwise changes legal status, it should obtain prior permission from the consumer before transferring the information to the new organisation. If the consumer does not grant permission, the information should be deleted.

All the above obligations must apply equally to any third party which receives personal information about a consumer, as well as to the original organisation that collects the information.

Access

Sites should provide users with access to all information held about them. Users should also be provided with information on systems which affect their legal rights through automatic processing (where a computer programme is used to make decisions about people). Users should be able to obtain this access speedily, and free of charge.

Sites should use methods to verify that such requests by consumers for access to data are genuine – to avoid giving out personal details to an impostor – but should not use such requests as an opportunity to gather yet more data.

An individual must be able to challenge the accuracy and completeness of their data and have it amended as appropriate. Sites should explain clearly how users can correct or delete their data.

Security

Organisations have an obligation to take both administrative and technical measures to ensure that information is collected, stored and transmitted in a secure manner. The level

of security should be appropriate to the sensitivity of the data collected.

Oversight and Compliance

An organisation should make specific information about its policies and practices relating to the management of personal information readily available to individuals

An organisation is responsible for personal information under its control and should designate an individual or individuals who are accountable for the organisation's compliance with its privacy principles.

An individual should be able to address a challenge concerning compliance with the privacy principles to the designated individual or individuals accountable for the organisation's compliance.

National governments should establish an independent oversight body to ensure compliance and provide for adequate sanctions for violations.

Redress

Consumers should have access to an independent redress mechanism that is cheap, quick and effective. Policymakers must give urgent consideration to the issue of redress in cross-border situations.

Privacy policies

All sites that collect information from users should provide a privacy policy that clearly states their policy towards that information.

The privacy policy should be signposted in a clear and prominent manner from the home page, and at every point within the site where personal information is collected.

The privacy policy should be written in a clear and easy to understand manner.

The privacy policy should include:

- the identity of the company that owns and operates the site
- the kind of information collected

- why the data is stored and what it is used for
- who the data is shared with (including a list of affiliates), and what choices the user has about this
- how long the data is stored for
- how the security of that data is ensured
- how consumers can access, alter and delete their data
- how the site's policy might change in the future
- contact details for the person responsible for the privacy of data
- contact information for the pertinent oversight body

Consumer action

Consumers should consider the existence and content of a privacy policy before submitting personal data to a site. This is particularly important when shopping from a site based in another country.

If consumers are concerned about privacy of their data, they should not use sites that do not adequately protect their data. In addition, they should consider tactics such as using a number of email accounts, or using a service that allows for anonymous browsing of the internet.

Consumers International have developed a practical tip sheet for consumers who want to protect their privacy online. See Appendix 6 for more details.

Children

Children and young people should not be encouraged to give information about themselves, their household or about any other persons. Giving information should not be made a condition of gaining access to the site.

Children and young people should not be offered rewards (money, gifts or anything else of a monetary value) for giving information.

Non-transparent methods of data collection (such as surveys and competitions) should never be used to collect information from children.

None of these policy recommendations are particularly radical, or call for anything that should not currently be common practice for companies. Indeed, in most cases, all Consumers International is calling for is that companies abide by existing legislation and guidelines regarding privacy of personal data.

Background

The internet has dramatically changed the world. An estimated 377 million individuals globally are now online.³ They are using the net to read news, talk to friends, buy goods, listen to music and for countless other activities. A significant number of people are using the internet to buy goods and services. As diverse networks of computers, telephones, television, cable and satellite merge, most activities in the developed world will be connected to online technology. A Forrester research survey estimates that US business to consumer internet sales will reach US\$108 billion by 2002.

When asked about their worries regarding online shopping, consumers have ranked invasion of privacy as a top concern. An American Express survey of 11,000 consumers in 10 countries found that 79 percent cited privacy and security as a major concern in relation to online shopping.⁴

This fear is turning many consumers away from using electronic commerce because they are concerned about the potential abuse of their personal information by electronic commerce companies. A survey by the US National Consumer League found that privacy was one of consumers' highest concerns. Fifty seven percent of the respondents said that they had not bought anything online in the last 12 months because they were worried that either their credit card number or their personal information would be abused. Other consumers reported that they provide false information to protect themselves.

Forrester research estimates that electronic-commerce sales were reduced by \$2.8 billion in 1999 because of privacy concerns.

While the technologies are developing at breakneck speed, the policies governing their use and the traditional protections that consumers have enjoyed for over a generation have lagged behind. In addition, new issues, such as defining jurisdiction and law in a world where transactions can easily occur between individuals in different countries and on different continents urgently need to be addressed.

Some technology is emerging to provide protection for consumers but the scope is limited. Even more confusing for consumers is the fact that frequently, privacy-invasive technology that actually encourages capturing of data is misleadingly promoted as protecting privacy.

Why this study?

This current research study grew out of a previous project coordinated by Consumers International and carried out by the same global research team. *Consumers@shopping: an international comparative study of electronic commerce*, published by Consumers International in September 1999, examined what happened when consumers bought a range of products over the internet. The aim was to find out how easy it was to shop on the internet, to identify problem areas, and to pinpoint good and bad practice. The shopping for this project was carried out in late 1998 and early 1999, and involved purchasing items both at home and abroad. A range of problems was identified. These included companies that provided inadequate information to the consumer; sent goods that arrived late or did not turn up at all; and delayed refunds.

One primary area targeted for criticism in the 1999 report was the sites' approach to data protection and privacy. Whilst almost all sites demanded certain pieces of personal information, only one in five explained to the consumer what use was made of this information. Most customers would expect to provide a minimum amount of information when buying something over the internet, but consumers do not necessarily want that information collected unless it is essential to the transaction. In particular, consumers do not want the information used for any purpose unrelated to the specific purchase they currently are conducting.

The findings of *Consumers@shopping* indicated a great deal of interest in the privacy aspect of electronic commerce, and demonstrated a clear need for more detailed research.

What is privacy?

Privacy is usually described as "the right to be left alone." It defines the relationship between an individual and society, including government, companies and other individuals.

Privacy is recognised as a fundamental human right in the Universal Declaration of Human Rights, adopted by the United Nations in 1948, and other international treaties. The range of issues that fall under the name of privacy is quite broad. These include secret communications and papers, protection of home and family, and bodily integrity.

In electronic commerce, the protection of privacy concerns the setting of rules and limits on the collection, handling, and use of personal information that is gathered by companies and other organisations as part of the interaction between a consumer and those companies. This is commonly referred to as "data protection".

Interest in data protection began in the 1960s with the increased use of computers in society. The collection and use of personal information by powerful computer systems prompted demands for specific rules governing the collection and handling of personal information.

Privacy, data protection and electronic commerce

Electronic commerce raises new concerns about privacy because the scope and detail of personal information collected about consumers is far greater than is usually collected in the off-line world.

The internet environment allows businesses to collect, analyse and use more information about customers, and with more ease and efficiency than ever before. The possibilities for storing, comparing, and linking information to build up a detailed picture of a customer's interests are huge. There have always been concerns over the way businesses use personal information, but the ease with which they can collect and manipulate that information on the internet makes the scale of the problem much larger. To add to the complexity of the situation, the internet has the potential for opening up markets – both for shopping and information-gathering – in other countries, which have widely diverse laws governing data protection.

There are important differences between how information is collected on customers who shop online versus those who shop the old-fashioned way – on the high street and in the malls.

Two of the most important differences are that most online companies keep track of users' visits and purchases. Unlike most consumer transactions off-line, detailed information is collected about individuals' actions even if they do not purchase anything. Secondly the consumer's name, address and perhaps even phone number – and often additional details as well – are collected for virtually every purchase as a condition of payment by credit card or for shipping purposes.

The computers that log all activities on their systems routinely capture all these particulars. The information ranges from the trivial to the most sensitive. In a typical electronic commerce transaction, this information would include not just the record of the items actually purchased but a list of all other others that were viewed.

Companies also often collect information from consumers in exchange for a free service, such

as news searches, free email and stock portfolios. In many cases, users are not informed that the information is being collected. Not surprisingly, however, those customer details are frequently fodder for targeting advertising.

Companies such as Netzero offer free net access in exchange for monitoring their users' activities for advertisers. Web sites known as "portals" offer personalised pages where a user can set up a free account to get selected news or stock quotes or chat with other users once they register and provide their names, addresses and interests.

A key concept in online marketing is personalisation. This is the belief that marketers can collect enough information about consumers to determine their desires for goods and to target specific advertising or other services at them. The perceived value of this information is what makes many of these dot.com companies worth so much on the stock market. The companies then sell, trade or share that information among third party companies without the consumer's express knowledge or consent.

Internet security and privacy

Internet security also raises serious concerns about privacy. Many web sites that retain personal information are poorly secured against accidental releases or deliberate attempts to penetrate computer systems for fraudulent purposes.⁵ At least one major security flaw in common software used by consumers and consumer-oriented businesses is discovered every week. It is common to have security breaches that result in the disclosure of personal information or financial records.

Many electronic commerce companies respond to concerns about security by stating that they are using encryption to scramble the communications between the user and the server – to prevent a third party from eavesdropping – when the user is providing sensitive information.

However, this protection is largely illusory. That information is highly vulnerable once it is collected and included on online databases.

Leaks of personal and credit card information occur daily, many involving hundreds of thousands of records. Thousands of customers of CDuniverse had to replace their credit cards after the database was stolen and offered for sale on the internet. In August 2000, Kaiser Permanente, a top US health insurer, admitted that it had compromised the confidentiality and privacy of its members when it sent over 800 email messages, many containing sensitive information, to the wrong members.⁶

In many cases, the consumer is not even aware that the information is on the net. Here are just two frightening examples: in Michigan, health information, including names, social security numbers and diagnostic codes of thousands of patients, was placed on the internet by the University of Michigan health care system and was publicly available for months. The US Social Security administration made their retirement database available on the internet in 1997 without any prior consultation.⁷

Spam

One manifestation of privacy invasions on the internet is the flood of unwanted electronic mail sent to consumers every day. Unsolicited commercial email, commonly known as "spam," is a major nuisance. Each day, millions of unsolicited electronic mails are sent to consumers. The Gartner Group estimates that 90% of all internet users receive one item of spam at least weekly and half receive six or more each week.⁸ It is estimated that the average consumer will receive 1,600 spam messages each year by 2005.⁹

Spam is an example of the failure to apply fair information practices. Addresses are purchased from electronic commerce companies and harvested secretly from web pages, discussion groups, and web chats. Consumer consent is not asked before the address is collected, used or transferred. Consumers have few options for reducing this problem. Once a consumer's email address is on a list, it is difficult to remove. Many spam messages do not have real return addresses. Even if there is a real address, many spammers take return messages to create new lists of verified email addresses that they can sell for a greater amount. It is also difficult to use

technical measures to filter out unwanted messages, since they come from thousands of different addresses. Much of the spam now arrives with misleading subjects such as “regarding your message”, to encourage consumers to read the email.

Spam clutters up consumers’ email boxes and makes it difficult to find important email. Many consumers are forced to change their email addresses and services to avoid spam. Some stop using the internet altogether because they are tired of receiving so much junk. Spam also costs the consumer money. In many areas around the world, the consumer must pay per minute or download charges to either the telephone company or the internet service provider. In addition, many internet service providers have to expend extensive resources hiring staff and buying additional equipment to deal with the flood of electronic mail they receive – and that cost is passed on to their customers. America Online (AOL) estimates that one-third of incoming mail to its servers – between 10 and 24 million messages each day – is spam. An industry association estimated in 1999 that \$2 of each customer’s bill could be traced to spam-related costs.

Marketers can also use spam to track user activities. Spam that is sent in html form and read by users of AOL or many other common email programs can send messages to advertising networks such as DoubleClick, linking consumers’ email addresses with their cookies (a cookie is a small file that is placed on the user’s hard drive. It contains a unique identifying number, and can be used to track what the user does when using the internet – see appendix 1 for more information). In the future, advertisers plan to combine marketing with mobile phone location so that marketers will be able to page or message customers on their phones to alert them to shopping opportunities – as they are passing selected restaurants, for example, or a sporting goods store. A more common practice is using spam to offer fraudulent schemes or pornography.

Privacy laws

The modern international benchmark for privacy protection can be found in the 1948

Universal Declaration of Human Rights, which specifically protects territorial and communications privacy. It also recognises that individuals have a right to legal protection against invasion of their privacy. Today, over 30 countries have comprehensive laws governing the processing and use of personal information. Another 20 countries are actively considering new laws.

A major milestone was the European Union’s (EU’s) adoption of data protection laws in 1995 and 1997 to harmonise laws throughout the EU to ensure consistent levels of protection for citizens and to allow for the free flow of personal information throughout the EU. The directives set a baseline common level of privacy which not only reinforced current data-protection law, but extended it to establish a range of new rights. The 1995 Data Protection Directive (Directive on the Protection of Personal Data (95/46/ec), which took effect in October 1998) set a benchmark for national law regarding processing personal information in electronic and manual files.¹⁰ The 1997 Telecommunications Directive established specific protection covering telephone, digital television, mobile networks and other telecommunications systems.¹¹

In all of the EU efforts, enforceability is a key concept. The EU is concerned that individuals have rights that are enshrined in explicit rules, and that they can go to a person or an authority empowered to act on their behalf. Every EU country has a data protection commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight. The directive imposes an obligation on member states to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the EU.

Many countries outside the EU have adopted similar laws. This is especially common in central and eastern Europe where many countries are attempting to join the EU and the Council of Europe. Numerous countries in the western hemisphere are also moving forward.

See appendix 2 for more detailed information on privacy laws.

Europe and the United States

Consumers International's main objective in coordinating this report was to compare the experience of consumers in the United States (US) and the European Union (EU) because there are major differences in approaches to regulation. Privacy practices are voluntary and business-led in the US. In the EU, many key consumer rights are enshrined both in EU and national legislation. Consumer organisations have expressed concern that EU consumers could be vulnerable to abuse of their personal data when buying from the US or using US-based websites.

Following the approval of the EU Data Protection Directive, many large American companies worried that they would be cut off from data flows from European countries because of the lack of laws protecting privacy in the US. The US government and industry strongly lobbied the EU and member countries to find the US system adequate.

In 1998, the US began negotiating a safe harbour agreement with the EU in order to ensure the continued trans-border flow of personal data. Negotiations on the drafting of the principles lasted nearly two years and were the subject of bitter criticism by privacy and consumer advocates¹² and the European Parliament¹³. In July 2000, despite the criticisms, the Commission approved the safe harbour agreement.¹⁴

Under safe harbour, US companies can voluntarily self-certify to adhere to a set of privacy principles loosely based on the fair information practices developed by the US Department of Commerce and the European Commission. These companies could then continue to receive personal data from the European Union. US companies have been able to join safe harbour from November 2000. However take-up has been remarkably slow, with only one company reportedly joining up as of early December 2000. There is an open-ended grace period for US signatory companies to implement the principles. The Commission promised to re-open negotiations

on the arrangement if the remedies available to European citizens prove inadequate.

There are many concerns that the proposal will not adequately protect consumers. A major weakness of the agreement is enforcement. The agreement rests on a self-regulatory system, whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. Individual consumers have no right to appeal or right to compensation for privacy infringements. The agreement will only apply to companies overseen by the Federal Trade Commission and Department of Transportation (excluding the financial and telecommunications sectors) and special exceptions are granted for public record information protected by EU law. It does not apply to internet or electronic commerce unless a European electronic commerce company transfers information about its customers to a US company that has signed up to the agreement.

To improve the arrangement, Consumers International recommends several changes. These include:

- the creation of a single point of contact for all consumer complaints with a simplified complaint system
- the establishment of biannual public reports on business compliance and the efficacy of the principles
- the creation of effective penalties including fines, restoration of privacy if possible, and compensation
- the establishment of an international e-commerce body with jurisdiction over privacy that could audit, set standards, promote best practices and publish reports.

Children and internet privacy

Parents, educators and many others have expressed considerable concern regarding the protection of children's privacy on the internet, especially because children are considered a lucrative target market for sales and online advertisers.

A groundbreaking report by the Center for Media Education entitled "*Web of deception*:"

*threats to children from online marketing*¹⁵ found that children were being targeted in two ways:

- 1) invasion of children's privacy through solicitation of personal information and tracking of online computer use; and
- 2) exploitation of vulnerable, young computer users through new unfair and deceptive forms of advertising.

The report found that sites were demanding detailed personal information including name, address, age and interests. Some sites told children that if they provided their name, address and other personal information, they would receive gifts such as t-shirts and games. Some sites made fun of the children who did not provide the information while allowing those who did to play games. A number of sites demanded detailed financial information about the parents.

Deceptive advertising is of particular concern with children. The report found that advertisers deliberately blurred the lines between advertising and information on children's sites. Advertising logos were often incorporated into cartoon characters designed to appeal to children and encourage them to demand these products.

Even something as apparently benign as companies working with schools to increase online access to children has a negative side.¹⁶ A company called Zapme in cooperation with other corporations including Amazon, Dell, Microsoft, Xerox and Yahoo offered free computers, satellite dishes, and internet access in exchange for gathering information about students. Students were required to get an electronic ID and to provide their names,

addresses and telephone numbers. The information was then provided to advertisers who targeted the students with individualised ads. The system was discontinued after a coalition of educators, consumer and privacy groups wrote to all of the governors in the US calling on them to reject the system. Other companies offered money to schools to encourage children to sign up for free accounts on their services.

In the United States, recognising these abuses, the US Congress approved the Children's Online Privacy Protection Act (COPPA) in 1998. The Act requires parental consent before information is collected from children under the age of 13 and allows parents to access information about their child.¹⁷

In order to assess companies' approach to privacy on sites targeting children, Consumers International assessed a small number of children's sites. One hundred and two sites were assessed in the US and EU. The findings indicate that the situation is still very worrying. Whilst a high number of companies are prepared to sell things to children online, very few seem to adhere to good privacy practice. The findings demonstrated that only a minority of sites (12%) had a clear, easy-to-understand privacy policy; even fewer (10%) asked children to obtain parental consent before disclosing information, asked children to tell parents they had given information to the site, or offered to email parents warning them that data had been disclosed. Although this exercise was small-scale, Consumers International feels this is a strong indication that sites targeting children are performing very poorly in their approach to privacy. This area merits a separate study in its own right.

The research

The project team

An international project team carried out the research. Researchers from 14 consumer organisations around the world carried out the assessments.

The full team met to discuss the findings and to agree to conclusions and recommendations.

List of participants

Australia	Australian Consumers Association
Belgium	Verbruikersunie
Denmark	Danish Consumer Council/Forbrugerradet
France	UFC-Que Choisir
Holland	Consumentenbond
Hong Kong	Hong Kong Consumer Council
Japan	Consumer Law News Network
Norway	Norwegian Consumer Council/Forbrukerradet
Poland	Polish Consumer Federation
Sweden	Konsumentverket
United Kingdom	Consumers Association And National Consumer Council
United States	American Council For Consumer Interests
Coordinator	Consumers International (ODTE)

Methodology

The research consisted of a large-scale assessment by users of internet sites. In total, the participants assessed 751 sites, based

mainly in the European Union and United States. The objective of the project was to determine the sites' approach to data protection, and therefore researchers concentrated on types of site where consumers would be likely to be asked to divulge personal information when shopping or searching for information. The participants researched *retail* sites, *financial* sites, *health*-related sites and in addition they looked at the *most popular* or heavily used sites on the web. Researchers also carried out a separate examination of sites targeted at children.

The category of *retail* sites covered businesses selling products to the consumer, and covered a wide range of companies including car dealers and restaurants as well as shops. Not all the sites within this category actually sold products online. Some provided information about their product range, store location, and offered catalogues online. The *financial* category included banks, insurance companies, money advice sites, online brokers, mortgage companies and credit unions. Not all of these sold their financial products online. The *health* category included general advice sites, doctors, dentists, and sites specialising in giving advice about one condition, hospitals, retailers of healthcare products, healthcare service providers and others. The *most popular* category covered a wide range of heavily used sites, including portal sites, email and internet access providers, news sites, weather sites, travel services, magazines, recruitment sites linked to television and radio stations, online directories, and games and leisure sites.

Rather than just visiting and assessing the biggest sites within each category, as this

might not give a complete picture of the internet world, the sites were chosen to represent a cross-section of those that consumers would come across when surfing the web. The project's findings offer a snapshot of the privacy situation on sites run by large, medium and small companies.

How sites were selected

Dun and Bradstreet, an internet listings firm, created a list of 300 US-based sites and 300 EU-based sites for each of the *retail*, *financial* and *health* categories. The project manager selected sites at random from Dun and Bradstreet's listings within each category. The list of EU sites was drawn proportionately to the total number of addresses for each EU country within Dun and Bradstreet's total pool. Researchers then worked their way down the lists, eliminating any sites that were not aimed at consumers.

For the *most popular* category, researchers provided a list of the top 100 sites in their country to the project manager, who then used a process of random selection to create a sample pool for the US and the EU. Sites were eliminated if they were not aimed at consumers, were pornographic, or were not accessible.

For children's sites, the sub-categories within the US site www.yahooligans.com were used and researchers were asked to provide a list of at least ten sites within each sub-category. The project manager then used random selection to create a sample pool of sites for each country in the study.

A total of 751 sites were assessed for the main study. The sites fell into the following categories:

<i>Health</i>	173
<i>Financial</i>	185
<i>Retail</i>	214
<i>Most Popular</i>	177
(not stated)	3)

Sites were based in the following countries:

USA	340
EU	339 of which:

UK	83
Denmark	86
France	25
Belgium	10
Germany	83
Sweden	52
Hong Kong	69

In addition, 102 questionnaires were completed about children's sites.

The number of sites assessed during this research is large enough for Consumers International to be able to draw conclusions with confidence about the state of data collection and protection in the US and EU at the time the research was carried out.

The assessments were carried out from March to July 2000.

Number of questionnaires completed by each organisation:

Australia	Australian Consumers Association	29
Belgium	Verbruikersunie	9
Denmark	Danish Consumer Council/Forbrugerradet	19
France	UFC-Que Choisir	25
Holland	Consumentenbond	68
Hong Kong	Hong Kong Consumer Council	119
Japan	Consumer Law News Network	65
Norway	Norwegian Consumer Council/Forbrukerradet	92
Poland	Polish Consumer Federation	31
Sweden	Konsumentverket	51
United Kingdom	Consumers Association	46
	National Consumer Council	24
United States	American Council For Consumer Interests	87
	Consumers' International	86

What our assessment covered

Consumers International wanted to find out whether it's possible for a consumer to browse sites and gather information without giving away information about him or herself.

Consumers International sought to determine what sort of information companies wanted to gather about consumers. Did they want the obvious information such as names and addresses; or did they ask for other details which consumers might consider more personal, such as age or occupation? Did these companies offer a choice about whether to provide this information, or was it compulsory if a customer wanted to use their sites?

Consumers International also wanted to investigate a company's approach to protecting the privacy of consumers' data.

Did the company have a privacy policy – a document that explains what it does with a customer's personal information and why? Did it give choices about whether a user wanted to be on the company's mailing list, or whether he or she wanted it to pass private details on to that company's associates or even to other unrelated companies? If the company did have a privacy policy, was it easy to find?

In addition to noting whether or not the company had a privacy policy, researchers assessed those policies, to judge how many of them presented consumers with adequate information and choices.

When visiting the site, the researchers established whether the site required consumers to divulge personal information in order to use it. If so, the researchers then completed a detailed questionnaire that looked at what information the site collected; whether it gave choices about what happened to that information; whether the site had a privacy policy; and what was in that privacy policy.

The researchers were asked to collect the following information:

- what sort of information the site asked for (e.g. name, address, date of birth, occupation); and whether this was compulsory or optional
- at what stage this information was collected

(did a customer have to give this information up-front before he or she could use the site, or only when he or she wanted to buy something or personalise the site)

- whether the site alerted the consumer to the company's privacy policy
- whether the consumer was able to opt out of mailing lists
- whether the site collected personal information in any other ways (e.g. surveys or competitions)
- whether the site had a privacy policy
- how easy it was to find the privacy policy
- what was contained in the privacy policy
- whether the site belonged to any sort of certification scheme
- whether the site explained its use of cookies
- whether the site gave information about security of payment systems

See Appendix 4 for a full version of the questionnaire.

The project's definition of information collection included any request for personal information either before or during the use of the site. Researchers noted any non-transparent methods of information collection such as surveys, competitions and feedback forms, in addition to all transparent methods. However, if the only way a site collected information was by providing an email address for feedback, and that email was voluntary on the part of customers and not related to their use of the site, then that site was classified as not collecting information about the user.

When searching for a privacy policy, researchers started by looking for a clearly-labelled statement that explained what the site did with information collected from the user. This might be called different things in different countries, but researchers were looking for something that explained what information is collected; what is done with that information; who it is shared with; what choices the user has about its use; and how security of that data is ensured. If researchers were unable to find a specific privacy policy, they carried out a key word search if possible. If that still failed to yield any information about the site's approach to privacy, they sent an email to the site asking it what its policy was.

What happens when consumers really shop using the internet?

The large-scale assessment of website practices and policies described in the previous section gives a good indication of what companies say they do with the personal information their customers give them. However, this may not always be what happens in practice. Consumers International wanted to find out whether companies always live up to their promises.

In order to test this out, researchers conducted a small investigative research exercise to better understand how privacy is protected and respected in a real internet shopping situation. This exercise is small-scale, so it offers no quantitative indication of website behaviour in general. However it gives valuable insight into potential problem areas.

A small team of researchers created a number of email “identities” to be used solely for this exercise. These researchers then made purchases on a range of sites in the USA and Europe (UK, Germany, France and Denmark). They bought a variety of products including books and CDs, pharmaceutical products, baby goods, chocolates and wine. They also made purchases on sites dedicated to weddings and fan clubs.

Whenever the site gave the consumer choices about including their name on a mailing list, the researcher made two purchases. Each purchase was made as a different person, using the unique email identities established at the outset. For one purchase, the researcher asked not to be included on any mailing lists for follow-up marketing, be it the company’s own mailing list, or a third-party list. The

researcher would then make a second purchase, using a second identity, and indicate that he or she was willing to receive further information in the future.

When a site did not offer a choice, researchers made one purchase only and noted the company’s policy on privacy and follow-up marketing.

Researchers then assessed whether the companies involved adhered to these requests, by tracking whether the identities received any further information or junk mail.

Researchers placed 52 orders in total, using 17 sites in the United States and 16 sites in Europe. Of these sites, 10 offered no choice about marketing follow-up; the rest did offer a choice. Orders were placed in October 2000. This report includes results of any follow-up mail sent until the end of November 2000. Of course, some companies may take some time to send out marketing material, and the process of selling names to third parties who then use those names for marketing purposes may take time as well. So this can only be an interim report, which hopefully will be followed with fuller findings.

Results

The majority of sites that gave consumers choice about whether or not they wanted their details used for mailing lists honoured those choices. Of the 21 identities that indicated they did not want any further information, be it from the company, its affiliates, or third parties, the majority did, in fact, not receive

any further mail – be it in electronic or postal format (at least so far). However, in three cases the company disregarded this request and sent their own email advertisements anyway. These sites were www.lalibrairie.com (a French site selling books and CDs), www.healthshop.com (a US site selling health products), and www.bbr.com (a UK wine retailer Berry Bros. & Rudd). www.bbr.com also sent regular mail to this identity. In one case an identity who purchased something from the US CD retailer www.cdnow.com received an email from a third party offering university diplomas for sale, although the same identity did not receive any emails from the company itself. It is possible that this third party site just sent out “blind” emails to names at this respective email provider address. However, none of our other identities using this email provider received a similar solicitation.

By comparison, of the 21 identities that did indicate they were willing to receive further mail of any sort, more than half of them (12) did receive email solicitations from the company itself. Only two received postal solicitations so far – one from www.thenutfactory.com (a US retailer specialising in dried fruits and nuts), and one, again, from www.bbr.com. Not a single one has so far received emails or postal mail from a third party.

Of the 10 identities that were not given a choice, seven did not receive any electronic or postal mail at all, while three did receive email solicitations. These were from www.harvard.com (a US bookseller), www.babyworld.co.uk (a UK retailer specialising in baby products), and www.rouge-blanc.com (a French wine retailer).

The conclusion reached by this exercise is that whatever a website’s privacy policy might say, a consumer cannot be absolutely confident that in all cases the site will adhere to this policy. In three out of 21 cases, websites used the customer’s personal details for marketing purposes despite the fact that the customer had explicitly chosen not to receive any such information. These results are based on monitoring over a short period – as time goes on, Consumers International may find even more companies breaching their promises to their customers.

A special opt-out procedure that seems to appear on many French websites raised an interesting point. The procedures made it very cumbersome for consumers to act on their right to opt out of mailing lists. Several of the sites tested did not provide the usual method of opting out of further emails – by ticking a certain box, for example, while placing an order. Instead, at some point during the transaction, the sites alerted consumers, although rarely in a prominent place, to their rights under Article 36 of the French Information & Liberty Law of 1978. In order to prevent a company from using the consumer’s information or from sending him or her further information in the future, it is necessary to send a postal letter to the company. This was the case with the sites www.lalibrairie.com and www.avecbebe.com. The two French sites www.rouge-blanc.com and www.nature-bio.com, notably did not make a reference to this law on their websites, nor did they provide opt-out choices.

Researchers also uncovered some worrying findings regarding security of payment card information. Researchers encountered various sites that did not have secure connections for the transmission of credit card and other personal details. Two of the most alarming examples involved two US sites.

In one case, www.3tee.com (a US t-shirt retailer) requested further information before finalising the order, through an un-encrypted email that included all the credit card and personal information the consumer had provided when placing the order (although the order itself was placed through an encrypted system).

In another case, the US CD retailer www.cdworld.com sent out two emails requesting further credit card confirmation details to be faxed to the company. They said they would not process the order unless they received this additional verification. However, in spite of the fact that researchers did not provide the company with this further verification, processed the order eventually. Interestingly, when the second identity placed the same order, using the same payment method, the company never requested further verification.

Results in detail

Did the site collect personal information? Just over two thirds of the sites assessed (67%) collected some sort of personal information about the visitor, at some point during the visit. Just under a third (32%) of the sites didn't ask for any information at any point during the visit.

Sites within the *most popular* category were most likely to gather something from the user, with 74% of sites visited collecting certain details. Sites within the *retail* and *financial* categories were close behind, with 73% and 70% of sites respectively gathering information. *Health* sites were least likely to collect anything, with 50% asking for information.

While the total percentage of sites collecting information is similar across the US and EU, there are some differences between findings for the US and EU sites within the categories. US-based *financial* sites are much more likely to collect information than EU-based *financial* sites. Researchers found that the US *financial* sites were much more likely to offer products and allow customers to apply online, which accounts for some of the difference. Within the *retail* category, many of the sites within the US sample were websites for local businesses (such as car dealers or restaurants) that gave details of their products but did not allow consumers to actually buy online. These type of sites did not appear as frequently in the EU *retail* sample. This explains why the sites in

the US *retail* sample are less likely to collect personal data than the sites in the EU *retail* category.

Table 1: site collects information

Total	US%	EU%
<i>Most popular</i>	80	72
<i>Financial</i>	84	48
<i>Retail</i>	61	79
<i>Health</i>	47	47
Overall total	66	63

Site tried to place cookie on the computer

Consumers International asked the researchers to set their browsers to alert them every time a cookie was placed. Just over a third of the sites visited tried to place at least one cookie. The vast majority of sites just placed one or two cookies, but a few placed up to fifty! US *most popular* sites were most likely to place cookies, with 92% of these sites visited in the survey placing at least one cookie.

Table 2: site placed at least one cookie

	US%	EU%
<i>Most popular</i>	92	47
<i>Financial</i>	22	24
<i>Retail</i>	30	32
<i>Health</i>	22	15

Table 3: What information did the site collect and was it compulsory or optional?

	Compulsory		Optional		Total	
	US%	EU%	US%	EU%	US%	EU%
Personally identifiable						
Name	50	74	44	24	94	98
Address	38	61.5	38	27	76	88.5
Email	43	60	42	30.5	85	90.5
Phone	36	35	34	41	70	76
Fax	5	7	11	25	16	32
Credit card debts	1	10	4.5	7	5.5	17
Demographic						
Postcode	37	57	42	27	79	84
City	37.5	58	40	26	77.5	84
Country	19	24	26	19	45	43
Date of birth	10	15	10	12	20	27
Occupation	6	6	9	6	15	12
Gender	1	5	1	2	2	7
Title	1	3	0	1	1	4

Almost all sites (99%) that gathered information collected some detail that would enable them to identify a user personally (for example, name, address, credit or social security card number). US *most popular* sites were the least likely to do this with 87.5% collecting something personally identifiable; all other categories did this between 96% and 100% of cases. Many sites also collected information that would enable them to know something about the user (and therefore possibly his or her spending habits), such as where you live, your address, age or occupation. In this way, many sites are able to build a profile of the customer in order to target their marketing activities.

Name, email name, and postal address details were the most commonly collected information across all sites. Age or date of birth, occupation, gender, fax details and credit card details were the other sorts of information that sites collected.

If a site collected information at all, it was quite likely to request a substantial amount of information from the consumer. Most sites collected between six and eight pieces of information.

At what stage was the information collected?

Only 15 of the sites researchers visited, or 7% of the total, insisted on receiving information before allowing a customer to visit the site.

It was most common to collect information after the user browsed the site, but before he or she made a purchase or requested specific information. This was true across all types of site, and is not surprising as many sites need to know certain things about the customer in order to respond to orders or requests.

US-based *most popular* sites were most likely to collect information before letting a user use the site – although this only happened in a minority of cases. The most-commonly asked question, appearing on 15 sites, was what country the customer was based in. This could be because the company needs to adapt the site in order to make it applicable to the country in which the user is located.

Did the sites have a privacy policy?

After searching thoroughly on each site, researchers were able to find a privacy policy for 292 (58%) of the sites visited that collected personal information.

Of sites that collected personal information from users, *health* sites were the least likely to have a privacy policy. US-based *most popular* sites were most likely to have a privacy policy, with all sites assessed in the study containing a privacy policy of some sort.

Most popular sites within EU and US-based financial sites also performed well.

Did the site alert the user to its privacy policy at the point where the information was collected?

If a site has a policy that explains what it does with the information supplied by the customer, the most obvious place to alert users to this is at the point where information is collected, rather than leave the user to hunt around for it.

Only a third (32.5%) of the sites that collected personal information and had a privacy policy bothered to alert the visitor to the privacy policy at the point where that information was collected. The only category of site that performed well in this respect was US-based *most popular* sites. Nearly two-thirds (62.5%) of these sites with privacy policies alerted users to them at the point where the information was collected.

How easy was it to find the privacy policy?

If a company has a privacy policy, supposedly for the benefit of consumers, it makes sense for this policy to be easily accessible. It is of little use to consumers if they cannot find it at the point when they need to read it. Ideally the privacy policy should be clearly signposted from the home page, in addition to being clearly marked at any point where data is collected from the user. However researchers found that this only happened in a minority of cases.

Researchers were signposted to the privacy policy from the home page in over a third (39%) of cases where sites collected information and had a privacy policy. US sites fared better than EU sites. In particular, *most popular* sites based in the US did far better than any other category – 97.5% of sites signposted their policies clearly.

Even when the privacy policy was signposted from the home page, it wasn't always easy to find. Researchers found that the privacy policy was prominent and easy to find in 63% of those sites where the policy was signposted from the home page – leaving 37% to do better.

If the privacy policy was not signposted from the home page, researchers were asked to attempt to find it by clicking around the site. One in five (20.5%) managed to find the privacy policy this way.

If they were still unable to find the privacy policy by clicking around the site, they proceeded to search within the site, using a search facility, if one existed. Although 18.5% of sites without an apparent privacy policy had a search facility, researchers only managed to find a privacy policy this way in two cases.

If, after all this searching, the researchers were still unable to locate a privacy policy, they emailed the sites to ask if they had a privacy policy. Researchers sent 177 emails inquiring if a privacy policy existed. Only 30 sites, or 17% responded. The sites' low response reflects a very poor performance, given the high level of consumer concern over privacy of personal data. As prompt response to emails is an essential part of building consumer faith in electronic commerce, it shows that many sites still have a long way to go to provide good customer service.

When companies did respond to the emails, the answers varied. The following responses are the most typical:

- the data is treated confidentially
- the data is not collected for any marketing purposes
- the data is not stored

Some sites misunderstood the question and gave answers that related to the way they encrypted data to ensure secure transmission. A few sites said they had plans to post a privacy statement on their site in the near future.

Were users given a choice about what purposes their data could be used for?

Companies may use customers' details for marketing purposes in a number of different ways. They may want to put those details on their own internal mailing list, in order to be able to send information about special offers or new products. They may want to pass the customer's name on to affiliates or associated companies. Or they might want to sell the

customer's name as part of a list to an outside company. Ideally consumers should be given the choice of opting in or out of all of these lists. Some companies have a stated policy of not passing personal details on to any other company, affiliated or otherwise. Nonetheless, they should still give consumers the option of not receiving promotional material from them.

European Union law requires companies that plan to use consumers' data for marketing purposes to give them the option of opting-out of this usage. There is no such requirement in the US. Despite this difference in legal requirement, researchers found that in general US-based sites were more likely to give users a choice about whether they wanted their details used or passed on for marketing purposes.

In general sites within the *most popular* category tended to perform better than other types of sites, both in the US and the EU. US-based *most popular* sites performed best of all. However all sites were very disappointing in the extremely low levels of choice given to users.

Did the site give you a choice about having your details put on their own mailing list?

Yes 20% No 80%

The only category that did relatively well was US *most popular* sites (57.5% gave a choice)

Did the site give you a choice about affiliates' mailing lists?

Yes 9% No 91%

Again US *most popular* sites did best (42.5% gave a choice)

Did the site give you a choice about third parties' mailing lists?

Yes 9.5% No 87% N/A 3.5%

Again US *most popular* sites did best (47.5% gave a choice)

Where were the opt-out choices given?

Information about the choices available to the consumer about how personal details are used should be accessible and transparent. These choices should ideally be presented prominently at the point where the user is asked for the information. Many users may not be aware that they might have a choice, so they might not look for such information.

Less than half (48%) of the small number of sites that gave opt-out choices offered them at the point where the data was collected. In just over a third (37%) of cases, researchers had to go into the privacy policy in order to find the opt-out choices.

Were other methods used to collect personal information?

Seventy-six (15%) sites attempted to collect data in other ways. Companies used competitions as the most common method of collecting information. Other methods included: surveys or feedback forms; invitations to send email comments on the site; and facilities to order a catalogue or join a club. Such methods of data collection can be a cause for concern if consumers are not clearly warned that personal information collected in this way will be stored and used by the site.

Certification schemes

Certification schemes are one effort to increase confidence in consumers shopping online. These schemes are essentially a stamp of approval or label given to internet sites which indicate that the companies operate within a certain set of approved standards. Some certification schemes are run by the industry, while others are independent and consumer-led. These "stamps of approval" should provide consumers with the confidence that they are shopping in a relatively safe environment.

Very few of the sites assessed in our study were part of a certification scheme. Those that were part of a certification scheme were almost all based in the US, where such certification programmes have existed for a longer time.

Sample sizes are too low to allow any comment on whether belonging to a certification scheme improves the site’s approach to privacy.

Content of privacy policy

Although having some sort of statement about what a site does with information is probably better than having nothing at all, many privacy policies are woefully inadequate. For users to be fully informed, the site should tell them: what information is collected and how it is used; what choices users have about the use of that data; what access users have to the data and how to amend it; how the security of that data is ensured; and who in the organisation is responsible for the data.

Researchers also looked to see whether sites told consumers how long they kept the data, and how their policy might change in the future. Although a site might have a very good privacy policy at the time the consumer uses the site, it could change in the future either because of a change of internal policy, or because that site gets taken over by another company. Ideally sites should warn customers of this possibility, and explain how they would inform the user of any significant changes to policy.

Whenever researchers came across a site with a privacy policy of any sort, they searched for these key aspects within the policy. Within this section, percentages refer to the total number of sites that both collected information about their users, and had some sort of privacy policy.

Researchers found that the content of privacy policies was very similar in both US and EU-based sites.

Information

What information is gathered about the customer?

Overall 39% of policies told customers this.

<i>most popular</i>	54%
<i>financial</i>	36%
<i>retail</i>	28%
<i>health</i>	17%

What is done with the information?

This was the most common feature of privacy policies of both US and EU-based sites, with 52% of policies giving information about this.

<i>most popular</i>	69%
<i>financial</i>	47%
<i>retail</i>	42%
<i>health</i>	33%

Why is information gathered about the customer?

This was the second-most-common feature of privacy policies of US and EU-based sites, with 48% of sites covering it.

<i>most popular</i>	61%
<i>financial</i>	49%
<i>retail</i>	35%
<i>health</i>	28%

Who is the information shared with and for what purpose?

Overall 42.5% of site policies covered this.

<i>most popular</i>	54%
<i>financial</i>	42%
<i>retail</i>	32%
<i>health</i>	22%

Choice

What choices are available to customers about what is done with their personal information?

Overall 17.5% told users about the options available to them.

<i>most popular</i>	26%
<i>financial</i>	16%
<i>retail</i>	12%
<i>health</i>	0

Can customers take their names off mailing lists in the future, and if so, how?

Overall 14% informed customers about this.

<i>most popular</i>	13%
<i>financial</i>	14%
<i>retail</i>	11%
<i>health</i>	17%

Access

Can consumers correct and update information about themselves, and if so how?

Overall 31% included this in their policies.

<i>most popular</i>	44%
<i>financial</i>	26%
<i>retail</i>	22%
<i>health</i>	22%

Can customers access information held about them, and if so, how?

Overall 18% of site policies covered this.

<i>most popular</i>	17%
<i>financial</i>	20.5%
<i>retail</i>	17%
<i>health</i>	11%

Can customers delete information, and if so, how?

Overall 16% of sites contained information about this.

<i>most popular</i>	24%
<i>financial</i>	11%
<i>retail</i>	11%
<i>health</i>	11%

Security

How is data security managed?

Overall 22% of site policies covered this.

<i>most popular</i>	20%
<i>financial</i>	26%
<i>retail</i>	22%
<i>health</i>	6%

Other aspects:

Is the name of the person responsible for data provided?

Overall 5% of policies included this.

<i>most popular</i>	6%
<i>financial</i>	4.5%
<i>retail</i>	5%
<i>health</i>	0

How long is information held for?

Overall 6% of policies included this.

<i>most popular</i>	8%
<i>financial</i>	0%
<i>retail</i>	7%
<i>health</i>	17%

Is there any guarantee of how long the site's policy will remain unchanged/might change in the future?

Overall 4% of policies included this.

<i>most popular</i>	5%
<i>financial</i>	4.5%
<i>retail</i>	2.5%
<i>health</i>	0

Generally the numbers of sites providing any of this key information were very low. Only US-based *most popular* sites stood out from the rest, with 88% telling the user what information is gathered about them; 85% saying why that information is gathered; 90% telling consumers what is done with that information; 78% telling consumers who that information is shared with and 66% telling consumers how to correct or update that information. In all other categories, sites performed very badly, with the vast majority failing to meet any of the important criteria needed for an adequate privacy policy.

This leads to the worrying conclusion that only a minority of sites that collect information actually tell the user anything about what the companies do with that information. Even when a policy is provided, in many cases it does not offer consumers the key information they need.

This failure on the part of the majority of sites is deeply worrying and, particularly since the guidelines on fair information practices in this area are well-established, shows a flagrant disregard for the concerns of consumers. Unless internet sites take a careful look at their privacy policies, they may well see consumer confidence – and willingness to use online services – erode over time.

Appendix 1: Cookies

Electronic commerce companies use numerous methods to identify and track consumers. One of the most common techniques currently used is the cookie. A cookie is a small file that is placed on a user's hard drive by a website. It contains a unique number generated by the site. The number is typically a series of numbers and letters intelligible only to the site but it may also contain the user's account name and password or Internet address.

Cookies were created by Netscape, an internet browser and server company, to improve websites' ability to track users over a single visit to a site. The cookie can also notify the site that the user has returned and can allow the site to track the user's activities across many different visits.

The use of cookies expanded greatly when it was realised that a single cookie could be used across many different sites by sending the cookie from a single third-party site. This led to the development of advertising network companies that track which users view which websites and develop profiles of their interests across many sites. These companies then use that information to target specific advertising. The cookies are not typically associated with a real identity. The largest ad service is DoubleClick, which has agreements with over 11,000 websites and maintains cookies on 100 million users, each linking to hundreds of pieces of information about the user's browsing habits. In 1999, DoubleClick bought a major US offline direct marketing firm and announced that it was going to start merging offline marketing data and user profiles. That announcement resulted in a storm of controversy and the plan has been stopped

for the time being. It also was revealed that DoubleClick received information about sensitive information – including health and financial details – about users through the placement of cookies.

A more secretive manner of tracking Internet users involves the use of web bugs, which are invisible images that also place cookies or report back that a user has visited a web site or read a specially formatted email. As of July 2000, DoubleClick had placed web bugs on over 60,000 different web pages.¹⁸ The bugs can also be used to merge cookies with email addresses.

There are more permanent methods of identifying users. In 1999, Intel announced that it was including a serial number in each new Pentium III chip that could be accessed by websites and internal corporate networks.¹⁹ Most of the manufacturers suppressed the number after a consumer boycott was announced, and Intel announced in 2000 that it is dropping the serial number in future chips. Soon after, several companies, including Microsoft and RealAudio, were discovered using the internal networking number found in most computers as another identifier.²⁰ The Internet Engineering Task Force has developed specifications for the next version of the Internet's underlying protocols called IPv6 that will assign a unique permanent ID number to every device hooked into the net, which could one day include common household devices such as refrigerators and VCRs.²¹

The growing use of wireless devices also raises serious concerns. Several US cellular phone providers disclose the user's phone number as

well as their Internet address when a customer uses their phone to access the Internet.

Growing numbers of programmes and devices exist that secretly monitor the activities of the user and send information back to the company that created it. In some cases, the software sends back a unique identifier. In others, such as with RealPlayer, the software sends a unique identifier and detailed information on the music that the user was listening to. Recently, readers of *Wired*, *Forbes* and other magazines were sent a free plug-in bar code scanner called the CueCat. Using the device, users can visit websites by reading bar codes in magazines and newspapers or that are encoded into television shows or ads. At the same time, the devices contain a unique ID number and maintain a detailed database of the users' activities. When hobbyists starting developing their own software that deleted the ID number and bypassed the corporate database, the companies' lawyers threatened them with violating intellectual property.

The convergence of communications networks, computers and mass media into an interactive network combining television and the Internet is the next progression of the technology currently being developed. Slowly, intelligent cable TV boxes, which can use broadband and interactive cable systems, are being deployed in many jurisdictions around the world. The new systems are being designed, like their Internet predecessors, to

track every activity of users as they surf the net through the boxes. They also are being designed to track the shows and commercials users watch and to use that information to tailor advertising for the greatest effect.²² The industry calls this "T-Commerce" for Television Commerce. Millions of consumers are expected to be using these in just the next few years, and the ad revenue to justify the new expensive boxes is expected to hit \$5 billion by 2004. Media titan Rupert Murdoch said of the box in a recent NewsCorp annual report, "It will tell us not only who our customers are, but what they buy, what they watch, what they read and what they want."²³

Unlike personal computers that give users control over their actions and choices, the new TV systems are generally based on a sealed "black box" controlled by the company that gives the user little or no control. In the WebTV box, users are not able to refuse cookies or delete them afterwards. The systems are closed and it is difficult, if not impossible, for even advanced users to identify what the system is doing. It will also prevent users from being able to use their own software. Meanwhile, there are other companies that have developed devices that will automatically record television shows for viewers and make recommendations for new shows based on viewers' previous behaviour. These systems also send some information on the viewers' habits back to the central offices.

Appendix 2: Privacy laws

An important facet in protecting privacy in electronic commerce and in other areas is law. The legal protection of privacy is deeply rooted in history going back to Biblical times. More recently, countries began adopting laws protecting citizens from the publication of their personal information. France prohibited the publication of private facts and set stiff fines for violators in 1858.²⁴ The Norwegian criminal code prohibited the publication of information relating to “personal or domestic affairs” in 1889.²⁵ In 1890, American lawyers Samuel Warren and Louis Brandeis wrote a seminal piece on the right to privacy as a tort action, describing privacy as “the right to be left alone.”²⁶ Following the publication, this concept of the privacy tort was gradually picked up across the US as part of the common law.

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy. It also recognises that individuals have a right to legal protections against invasions of their privacy.

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. National laws in Sweden (1973), the United

States (1974), Germany (1977), and France (1978) followed this.²⁷ Today, over 30 countries have comprehensive laws governing the processing and use of personal information. Another 20 countries are actively considering new laws. Most countries around the world have sectoral laws protecting privacy in some aspect or another.

A major milestone was the European Union’s adoption of data protection laws in 1995 and 1997, to harmonise laws throughout the EU in order to ensure consistent levels of protections for citizens, and to allow for the free flow of personal information throughout the EU. The Directives set a baseline common level of privacy which not only reinforce current data protection law, but extended it to establish a range of new rights. The 1995 Data Protection Directive set a benchmark for national law for processing personal information in electronic and manual files.²⁸ The 1997 Telecommunications Directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems.²⁹

In July 2000, the European Commission, issued a proposal for a new directive on “the processing of personal data and the protection of privacy in the electronic communications sector.”³⁰ It will replace the existing 1997 Telecommunications Directive by extending the existing protections for an individual’s “telecommunications” to a broader, more technology-neutral category of “electronic communications.” These new provisions would, for example, ensure the protection of all information (“traffic”) transmitted across the Internet, prohibit unsolicited commercial marketing by e-mail (spam) without opt-in

consent, and protect mobile phone users from precise location tracking and surveillance. The directive also gives subscribers to all electronic communications services (such as GSM and e-mail) the right to choose whether they are listed in a public directory.

In all of the EU efforts, enforceability is a key concept. The EU is concerned that data subjects have rights that are enshrined in explicit rules, and that they can go to a person or an authority empowered to act on their behalf. Every EU country has a Data Protection Commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight. The Directive imposes an obligation on Member States to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the EU.

Many countries outside the EU have adopted similar laws. This is especially common in Central and Eastern Europe where the countries are attempting to join the EU and the Council of Europe. Many countries in the Western Hemisphere are also moving forward. In Canada, the Federal Parliament approved Bill C-6, the Personal Information Protection and Electronic Documents Act in April 2000.³¹ The Act adopts the Canadian Standards Association's International Privacy Code into law for enterprises that process personal information "in the course of a commercial activity," and for federally regulated employers with respect to their employees. In three years, the Act will cover provincially regulated sectors unless the province enacts "substantially similar" laws, such as Québec's law. Laws based on the EU Directives have also been approved in Chile and Argentina. In Asia, Hong Kong and Taiwan have already adopted laws and nearly a dozen other countries are actively considering new laws on data protection.

Sectoral Laws

Some countries, such as the United States, have avoided enacting general data protection rules in favour of laws governing specific areas such as medical or financial records. In such

cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology, so protections frequently lag behind. The lack of legal protections for medical and genetic information in the US is a striking example of its limitations. There is also the problem of a lack of an oversight agency. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.

Other countries such as South Korea and Mexico have adopted specific laws on electronic commerce that also protect privacy.

Self Regulation

Another possible method for protecting privacy is through industry self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. Self-regulation has different meanings in the US and Europe. In the US, which lacks a comprehensive privacy protection law, industry is not required to follow any minimal standards and there is little evidence that the aims of the codes are regularly fulfilled. There is also a serious problem with enforcement.

In Europe, there is discussion of self-regulation, but in the EU context, self-regulation usually means that industry develops codes based on the standards in the national data protection laws and enforcement is ensured by the national data protection agencies.

In an effort to promote self-regulation, industry is focusing on adopting website privacy policies that provide some information to consumers on what details are collected and how they are used and disclosed. Most major e-commerce sites in the United States have adopted these policies.

Consumers have found numerous problems with these policies. Of primary concern is that in an unregulated environment such as the United States, there is no minimum standard for the policy. Many of the privacy policies

simply state that they are collecting a great deal of information about users and that they are planning to use that information for unknown purposes at their discretion and disclose that information to an unknown number of outside organisations for unknown reasons. A number of surveys by the US Federal Trade Commission and independent groups such as EPIC, in addition to this study by Consumers International, have found that most privacy policies do not adequately protect privacy.

Because there is no legal framework, the privacy policies can be changed at will by the company. Bookseller Amazon.com recently changed its policy from promising never to sell the personal information of its customers to notifying users that it may do at some point in the future. DoubleClick went from offering a semi-anonymous system to an attempt to

merge their online records with personal information from offline.

Problems also arise when the legal status of a company changes. If a company goes bankrupt or is bought by another company, the privacy protections of the policy are in doubt. The information can also be placed in the public record because it is frequently the only asset of the company. When Living.com filed for bankruptcy, the trustee placed the names and addresses of thousands of customers on the web.

Finally, enforcement of privacy policies in countries without laws such as the United States is limited. At best, the consumer can ask the Federal Trade Commission or state Attorney General to enforce the promises. Not surprisingly, this works very infrequently.

Appendix 3: Technologies of privacy

Tools are available that can protect the privacy of users in many cases. These technologies are known as “Privacy Enhancing Technologies” (PETs) and include anonymous web browsers, remailers and encryption. The European Commission in 1998 looked at some PETs and stated that the tools would not replace a legal framework but could be used to complement existing laws.³²

Encryption has become the most important tool for protection against surveillance. A message is scrambled so that only the intended recipient will be able to unscramble, and subsequently read the contents. Pretty Good Privacy (PGP) is the best-known encryption program and has hundreds of thousands of users, including human rights groups.³³ An open source program called GNU Privacy Guard is being developed as a free replacement that will allow anyone to view the full source of the system to ensure that it does not allow for secret surveillance.³⁴

“Anonymous remailers” strip identifying information from e-mails and can stop traffic analysis. They have generated opposition from police and intelligence services. In Finland, a popular anonymous remailer had to be shut down due to legal challenges that forced the operator to reveal the name of one of the users. More advanced tools that merge the functions of anonymous remailers and encryption have also been developed. The Mixmaster anonymous remailers used encryption links between anonymous remailers to hide the identity of the original sender by sending the message randomly through a series of remailers before delivering it to the final destination.

Another useful tool allows consumers to browse anonymously. Many of these services also prevent cookies, or applications that can be used to spy on the consumer from being placed on the consumer’s computer. The most sophisticated ones, such as Freedom.net, provide a fully encrypted link between the user and secure servers run by the company to prevent wiretapping, and encrypted headers so that users can receive email and browse the Internet without even the company knowing who is using the system.

Limits of technology

Users should be aware that not all tools are effective at protecting privacy. A major limitation is that almost none of the tools address the protection of privacy once the information is collected. Encryption is useful for ensuring that personal information is protected in transit but this says nothing about how the information is used by the companies once it collected.

Industry also offers many tools that are not privacy-protective. Many of these systems, such as Microsoft’s Passport and the World Wide Web Consortium’s (W3C) Platform for Privacy Preferences (P3P), are designed more to facilitate data sharing than to protect users.³⁵ They are also frequently used by US industry as justification for not passing laws.

Marketing hype frequently promotes tools as privacy protective that have nothing to do with privacy. American Express announced in October 2000 its Private Payments program, which would allow for the creation of one-time credit card numbers for online purchases.

The card number would have the effect of preventing users from having their cards stolen and used for other purposes but personal information would still need to be transferred to the merchant and Amex

would still have a record of the purchase.

Finally, many tools are not secure. Some are poorly designed while others may be designed to facilitate law enforcement access.³⁶

Appendix 4: The questionnaire

In which country is the site based: _____

Type of site (e.g. retail, health, financial, most popular): _____

Date you completed the questionnaire: _____

Re sites in the 'Most Popular' category:

Did you already assess the site in a different category?

Yes (which one) _____ No

If you have already assessed a site in a different category, do not go through the whole assessment procedure again. Instead, copy your replies on to the questionnaire for the category 'Most Popular'. (The site still counts as one in this category so we need the information).

1 Personal information collected by the site

1.1 Site collects no personal information

If the site collects no information at all about you, please just tick here and do not complete the rest of the questionnaire.

If the site collects any information about you, please tick and continue.

Site tried to place cookie on my computer (if applicable write here how many times)

1.2 What information does the site collect, and is it compulsory or optional? (Please tick the relevant answer)

Name	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Address	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Postcode	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
City	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Country	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Email name	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Phone number	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Date of birth	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Occupation	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Fax number	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Credit card number	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>
Card expiry date	Compulsory <input type="checkbox"/>	Optional <input type="checkbox"/>	Not collected <input type="checkbox"/>

Other (please list e.g. gender, number of children, marital status, income; and specify whether compulsory or optional)

1.3 Please describe at what stage the information was requested from you:

Before being able to use the site

After browsing the site but before making a purchase or requesting specific information

Before being able to “personalise” the site

Address

Postcode

City

Country

Email name

Phone

Date of birth

Occupation

Fax number

Credit card number

Card expiry date

Address

Postcode

City

Country

Email name

Phone

Date of birth

Occupation

Fax number

Credit card number

Card expiry date

Address

Postcode

City

Country

Email name

Phone

Date of birth

Occupation

Fax number

Credit card number

Card expiry date

1.4 At the point where this information was collected, did the site alert you to the privacy policy?

Yes

No

1.5 Did the site give you the option of opting-out of their own mailing list (e.g. not receiving information or special offers from them)?

Yes

No

1.6 Did the site give you the option of opting-out of having your details passed on to partners/subsidiaries/affiliates (associated or attached as a member or a branch to the main company)?

Yes

No

1.7 Did the site give you the option of opting-out of having your details passed on to outside parties (completely different companies that don't have any links to the company whose site you are assessing) (N.B. some sites will refer to outside parties as third parties)?

Yes

No

1.8 Were you presented with these opt-out choices at the point where your personal information was collected (i.e. on the same or next screen) or did you have to click on the privacy policy in order to become aware of and use these choices?

On the same/next screen

Had to go into privacy policy

Other (please describe) _____

1.9 In addition to the transparent collection of your personal information, did you notice any other methods by which the site attempted to collect personal data (e.g. surveys or competitions)?

Yes (please describe) _____

No

1.10 Please provide any other information you feel is relevant here, or any other types of opt-out given that were not listed previously.

2 Information about the privacy policy

2.1 Starting at the Home Page (this may be the very first page of a site or may be reached after clicking site's logo): Are you alerted to the privacy policy from the home page?

- Yes No

2.2 If yes, would you say that the way they alerted you to the privacy policy was:

- Prominent and easy to find
 Not so easy to find – had to look hard for it

2.3 If No, try clicking around the site to find the privacy policy. Could you find a privacy policy in this way?

- Yes No

2.4 If Yes, where was the policy located?

How many clicks away from the Home Page was this?

2.5 If No, please try searching for 'privacy policy' using the search engine on the site, if one exists.

Did the site have a search facility?

- Yes No

2.6 Were you able to find the privacy policy in this way?

- Yes No

2.8 If No, please email the website to ask if they have a privacy policy. Email sent (date): Reply received (date and please enclose a copy of the reply marked with you name and organisation and the name of the website as you have specified it on this questionnaire):

2.8 **Is the site a member of a certification programme?**

Examples of such certification programmes are: Trust.e – an independent, non-profit initiative whose mission is to build users’ trust and confidence in the Internet by promoting the principles of disclosure and informed consent. CPA WebTrust – a seal of assurance for electronic commerce which meet the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) defined criteria for standard business practices and controls over transaction integrity and information protection.

- Yes (please specify which one) _____
- No

Any other comments at this stage? _____

3 **The privacy policy**

Please go into the site’s privacy policy in order to complete the following section.

3.1 **If no privacy policy exists please tick below and move on to section 4. on ‘cookies’.**

- No privacy policy exists

3.2 **If the site does have a privacy policy, does the privacy policy tell you:**

- What information is gathered about you
- Why that information is gathered about you
- What is done with the information
- How long that information is held for
- Who your information is shared with and for what purpose
- The choices available to you about what is done with your information
- If and how you can access the information held about you
- If and how you can correct or update the information
- If and how you can delete the information
- If and how you can unsubscribe from mailing lists in the future
- Any guarantee for how long the site’s policy will remain unchanged, or information about how it might change in the future.
- The name of a person responsible for control of this data
- How security of data is managed

Please feel free to add any information you feel is relevant:

4 **Cookies**

4.1 **Did the site explain their use of cookies?**

- Yes
- No

4.2 What cookies were placed by the site?

4.3 To your knowledge, were any cookies placed by any other site than the site you were currently assessing?

Yes

No

5 Security of payment information

5.1 Does the site give any information about the security of the information you provide in order to pay for goods or services (e.g. credit card details)?

Yes

No

6 Conclusion

Thank you for your time and effort in completing this survey. Please take a moment to express how your interaction with this site made you feel about your privacy (e.g. did you feel your privacy was completely protected? Appropriately respected? Invaded? Or you didn't care about privacy so long as the site met your other needs?). Feel free to add more pages if you need.

Appendix 5: The participants

Australia

Australian Consumers' Association (ACA)

57 Carrington Road
Marrickville NSW 2204
Australia

Tel: +61 29 577 3333

Fax: +61 29 577 3377

E-mail: ausconsumer@choice.com.au

Web site: <http://www.sofcom.au>

Zara Baxter

Belgium

Association des Consommateurs/ Verbruikersunie (VU)

Test Achats
13 Rue de Hollande/Hollandstraat
1060 Brussels
Belgium

Tel: +32 2 542 3211

Fax: +32 2 542 3505

E-mail: abonnement@test-achats.be

Web site: <http://www.test-achats.be>

Françoise Domont-Naert

Denmark

Forbrugerrådet

Danish Consumer Council

Fiolstraede 17
DK-1017 Copenhagen K

Tel: +45 77 41 77 41

Fax: +45 77 41 77 42

E-mail: fbr@fbr.dk

Web site: <http://www.fbr.dk>

Annette Højrup

France

UFC-Que Choisir
11, rue Guénot
75555 Paris
Cedex 11

France

Tel: +33 1 43 48 55 48

Fax: +33 1 43 48 4435

E-mail: mouvement@quechoisir.org

Web site: <http://www.quechoisir.org>

Nicholas Larmagnac

Hong Kong

Hong Kong Consumer Council (HKCC)

GPO Box 191

North Point

Hong Kong

China

Tel: +852 2856 3113

Fax: +852 2856 3611

E-mail: cc@consumer.org.hk

Web site: <http://www.consumer.org.hk>

Vera Tam

Germany

The research on Germany was carried out by
CI staff.

Marcus Lenzen and Heiko Habbe

Japan

Consumer Law News Network (CLNN)

Ueda Katsuhiko Law Office
Osaka Bengoshi Building 409
6-7-4 Nishi Temma, Kita-Ku
Osaka 530 - 0047

Japan

Tel: +81 66 362 8177

Fax: +81 66 362 8178

E-mail: uedalaw@skyblue.ocn.ne.jp

Takeshi Muramoto

Netherlands

Consumentenbond

Enthovenplein 1
P.O. Box 1000
2500 BA The Hague
The Netherlands
Tel: +31 70 445 45 45
Fax: +31 70 445 45 90
E-mail: klantenservice@consumentenbond.nl
Web site: <http://www.consumentenbond.nl>

Perry Perfors and Janneke Stokroos

Norway

Forbrukerrådet

The Consumer Council of Norway

Postboks 123
N-1325
Lysaker
Norway
Tel: +47 67 599 600
Fax: +47 67 583 606
E-mail: post@forbrukerradet.no
Web site: <http://www.forbrukerradet.no>

Eli Rekstad

Poland

Federacja Konsumentów

Polish Consumer Federation

Pl. Powsta_ców W-wy 1/3
00-030 Warsaw
Poland
Tel: +22 827 51 05
Fax: +22 827 51 05
E-mail: biuro@federacja-konsumentow.org.pl
Web site: <http://www.federacja-konsumentow.org.pl>

Monika Kosinska

Sweden

Konsumentverket/KO

National Board for Consumer Policies/The Consumer Ombudsman

S-118 87 Stockholm
Sweden
Tel: +46 8 429 0500
Fax: +46 8 429 8900
E-mail: kosumentverket@kov.se
Web site: <http://www.konsumentverket.se>

Ingela Allenbert

United Kingdom

Consumers' Association (CA)

2 Marylebone Road
London NW1 4DF
UK
Tel: +44 20 7830 6000
Fax: +44 20 7830 6220
E-mail: which@which.net
Web site: <http://www.which.net>

Michelle Childs

National Consumer Council (NCC)

20 Grosvenor Gardens
London SW1W 0DH
UK
Tel: +44 20 7730 3469
Fax: +44 20 7730 0191
E-mail: info@ncc.org.uk
Web site: <http://www.ncc.org.uk>

Alison Hopkins

United States

American Council on Consumer Interests (ACCI)

240 Stanley Hall
University of Missouri
Columbia, MO 65211-0001
USA
Tel: +1 573-882-3817
Fax: +1 573-884-6571
E-mail: info@consumerinterests.org
Web site: <http://consumerinterests.org>

Robert Mayer

Observer

Bureau Européen des Consommateurs (BEUC)

European Consumers Organisation

Avenue de Tervueren 36 Bte 4
1040 Brussels
Belgium
Tel: +32 2 743 1590
Fax: +32 2 735 7455
E-mail: consumers@beuc.org
Web site: <http://www.beuc.org>

Ursula Pachtl

Appendix 6: Five steps to protecting your privacy online

– A consumer tip sheet

❶ Limit the disclosure of your personal information

Only provide information necessary to conduct the transaction. Do not give information such as biographical information that is not compulsory. Use a pseudonym when possible. If you think that a site is demanding too much non-essential information, vote with your mouse and use another site.

Prevent your software from disclosing information about you. These include the “Forms Autocomplet” function in Internet Explorer and the “Smart Browsing” feature in Netscape. You may turn these off in the “Preferences” menu option. Many other programs including word processors, games and Internet programs also frequently send information about the user back to companies. A list of this software and programs to remove them is available at <http://grc.com/optout.htm>

Be aware that when you put a message on newsgroups, chatrooms, web sites and other places on the net, the information is frequently stored and made publicly available.

❷ Set up a separate email account

Set up free email accounts separate from your personal or business account that you use only for electronic commerce or only for newsgroups, chatrooms etc. A directory of free email services is available at <http://www.emailaddresses.com/>

If one of your accounts starts getting a lot of unsolicited mail from companies or others, you can easily delete it and get another free account. Some of the services are also anonymous, and are encrypted to prevent anyone from reading your mail.

❸ Reject cookies

Set your browser to reject all cookies, or at least all third party cookies from companies like DoubleClick.

You can do this using a setting under “Preferences” in Internet Explorer and under “Preferences: Advanced” in Netscape. Only a few sites require cookies. For those sites, temporarily enable the cookies and then delete them when you are done. You can also use a program that will delete or edit your cookies files as you desire.

❹ Use tools to protect privacy

There are many tools that can be used to protect privacy. Your computer frequently discloses information about you. The French Commission Nationale de l'Informatique et des Libertés has a demonstration and information in English, French and Spanish at <http://www.cnil.fr/traces/index.htm>.

Users can also protect their privacy by using services that allow for anonymous surfing of the internet to prevent web sites from collecting information about you; encryption to protect the privacy of your communications; firewalls to prevent your computer from disclosing information about to others; and utilities for permanently erasing files and personal information on your computer. A list of tools is available at <http://www.epic.org/privacy/tools.html>

❺ Learn about your legal protections

Many jurisdictions have laws that protect consumers' privacy. You can see an analysis of many countries' privacy laws at <http://www.privacyinternational.org/survey/>. Many countries have a local or national official who is charged with protecting privacy and can assist you if your privacy is invaded. A full list of offices is available at the Council of Europe's web site at: <http://www.coe.fr/dataprotection/eautorites.htm>

To download a copy of Consumers International's report “Privacy@net”, go to www.consumersinternational.org. You can also print out more copies of this sheet. Both are available in French and Spanish.

Footnotes

¹ OECD, “Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data” Paris, 1981. <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>.

² Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. <<http://www.coe.fr/eng/legaltxt/108e.htm>>.

³ Nua Internet Survey’s < http://www.nua.ie/surveys/how_many_online/>.

⁴ <http://home3.americanexpress.com/corp/latestnews/gis2000/gis2000.pdf>.

⁵ See eg. Eric Murray, SSL Server Security Survey, July 31, 2000 showing that encryption on most e-commerce sites is inadequate. <http://www.meer.net/~ericm/papers/ssl_servers.html>.

⁶ See, “Sensitive Kaiser E-Mails Go Astray,” Washington Post, August 10, 2000.

⁷ See <http://www.epic.org/privacy/databases/ssa/>.

⁸ <http://www.brightmail.com/global/pdf/gartner.pdf>.

⁹ Jupiter Communications, E-mail Marketing to Soar to \$7.3 Billion in 2005 Cannibalizing 13 Percent of Direct Mail Revenues, May 8, 2000.

¹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>.

¹¹ Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997), <<http://www.ispo.cec.be/legal/en/dataprot/protection.html>>.

¹² See for example the Statement of the Transatlantic Consumer Protection Dialogue on U.S. Department of Commerce Draft International Safe Harbor Privacy Principles and FAQs March 30, 2000, <<http://www.tacd.org/ecommercef.html#usdraft>>.

¹³ European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. <http://www.epic.org/privacy/intl/EP_SH_resolution_0700.html>.

¹⁴ Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf>.

¹⁵ Available at <http://www.cme.org/children/marketing/deception.pdf>.

¹⁶ Center for Advanced Technology in Education, Capturing the “Eyeballs” and “E-wallets” of Captive Kids in School: Dot.com Invades Dot.edu <<http://netizen.uoregon.edu/documents/eyeballs.html>>.

¹⁷ FTC Privacy Pages, <<http://www.ftc.gov/privacy/index.html>>.

¹⁸ To find the number of web bugs used on pages by Internet advertisers, see <http://www.tiac.net/users/smiths/privacy/wbfind.htm>.

¹⁹ See <http://www.bigbrotherinside.org/>.

²⁰ See Richard Smith, Internet Privacy Issues. <<http://www.tiac.net/users/smiths/privacy/index.htm>>.

²¹ See <http://www.junkbusters.com/ht/en/new.html#IPv6>.

²² See David Burke, *Spy TV* (Slab-O-Concrete Press, 1999). <<http://www.spyinteractive.com/spyinteractive/>>.

²³ Cited in *Privacy Journal*, October 1999.

²⁴ The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris*, 68 *Tul. L. Rev.* 1219 (May 1994).

²⁵ See prof. dr. juris Jon Bing, *Data Protection in Norway*, 1996. <http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html>.

²⁶ Warren and Brandeis, *The Right to Privacy*, 4 *Harvard Law Review* 193 (1890).

²⁷ An excellent analysis of these laws is found in David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press 1989).

²⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>.

²⁹ Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997), <<http://www.ispo.cec.be/legal/en/dataprot/protection.html>>.

³⁰ European Commission, 'Proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector' <http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf>.

³¹ Bill C-6, *Personal Information Protection and Electronic Documents Act* <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.

³² Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp11en.htm>.

³³ PGP International Page: <http://www.pgpi.com/>.

³⁴ Homepage: <http://www.gnupg.org/>.

³⁵ EPIC and Junkbusters, 'Pretty Poor Privacy: An Assessment of P3P and Internet Privacy', June 2000, <<http://www.epic.org/reports/prettypoorprivacy.html>>.

³⁶ EPIC maintains a list of tools at <http://www.epic.org/privacy/>.

Consumers International
Office for Developed and Transition Economies (ODTE)
24 Highbury Crescent
London N5 1RX, UK
Tel: +44 020 7226 6663
Fax: +44 020 7354 0607
e-mail: odte@consint.org
Web site: <http://www.consumersinternational.org>



Consumers International

About Consumers International

Founded in 1960, Consumers International (a non-profit organisation registered in The Netherlands as the International Organisation of Consumer Unions, registration number S1 49999) is a federation of consumers' organisations dedicated to the protection and promotion of consumers' interests worldwide through institution building, education, research and lobbying of international decision-making bodies. An independent, non-profit foundation, Consumers International has 225 members in over 260 countries.

Head Office, 24 Highbury Crescent, London, N5 1RX, UK
Tel: +44 171 226 6663 Fax: +44 171 354 0607
Asia and the Pacific, Lot 5-1 Wisma WIM, 7 Jalan Abang Haji Openg
Taman Tun Dr. Ismail, 60000 Kuala Lumpur
Tel: +60 3 7726 1599 Fax: +60 3 7726 8599 e-mail: consint@ciroap.org
Latin America and the Caribbean, Casilla 9635, Santiago, Chile
Tel: +56 2 335 1695 Fax: +56 2 231 0703 e-mail: consint@entelchile.net
Africa, Private Bag A6215, Avondale, Harare, Zimbabwe
Tel: +263 4 302 283 Fax: +263 4 303 092 e-mail: roaf@harare.iafrica.com