

Privacy toolkit

An international business guide
for policymakers

Published in November 2003 by

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

38 cours Albert 1er
75008 Paris, France

Copyright © 2003

International Chamber of Commerce

All rights reserved. No part of this work may be reproduced or copied in any form or by any means – graphic electronic or mechanical including photocopying recording, taping or information retrieval systems without written permission of ICC.

FOREWORD

By Christopher Kuner, Chairman, ICC Task Force on the Protection of Personal Data; Partner, Hunton & Williams, Belgium

There is no 'one size fits all' privacy regime that will work for every country. Differences in national political cultures, economies and legal systems mean what works for one country may not suit another. But optimal privacy regimes do share some characteristics; they are flexible and robust, and let the interaction of consumer empowerment, technology, and business processes put agreed privacy principles into everyday practice.

Balancing the values of individual privacy with the drive for an open and competitive economy is not about achieving a fixed and timeless legal solution. It's an ongoing process that needs to be responsive to new technology, business methods and opportunities, and, above all, that actively engages all stakeholders. I hope the *ICC Privacy Toolkit* will show that the most important aspect of privacy protection is not how it is achieved, but simply that it works.

TABLE OF CONTENTS

Foreword	3
Introduction	7
ICTs and economic growth	8
Benefits of flexible privacy protection	9
Functions of privacy protection	11
Privacy principles	13
Implementing privacy protection	15
Overly restrictive privacy protection	18
Action items for governments	21

INTRODUCTION

Effective and appropriate privacy protection is a business enabler, not a barrier. It is a way to ensure consumer confidence and trust, and an enabler of lasting and fruitful customer relationships. Global business supports the use of a wide range of privacy enabling measures, and recognizes that there is no 'one size fits all' approach to privacy protection.

ICC has created this document with two purposes in mind: first, it can be used by national committees and members in discussions on privacy with their governments to ensure that any privacy regime adopted allows business and consumers to enjoy the benefits of privacy protection while at the same time enabling economic growth. Second, it can be used by ICC national committees to inform member companies about data protection law and other alternatives to managing privacy.

This Toolkit sets out the business context for privacy protection and describes the characteristics and benefits of optimal privacy protection regimes. ICC advocates consensus on principles for the use of personal data, and flexibility on the many mechanisms that can be used to apply these principles and ensure compliance. This Toolkit points out the potential adverse effects of relying too heavily on overly burdensome and legislation-centred approaches to privacy protection. It concludes with a set of action items for governments to promote appropriate and effective privacy protection regimes.

ICTs AND ECONOMIC GROWTH

The evolution from a manufacturing-centred to a services-centred economy since World War II tracks the development of digital technologies. These technologies have made it possible to collect, process, store, understand and apply information in ever more useful and robust ways. In addition, analyzing data from the manufacturing process made it possible to find new solutions to old industrial age problems. Computer-aided design, and computer-aided manufacturing and inventory controls in the 1970s and 1980s revolutionized quality, reduced prices, and stimulated competition as companies continued to innovate.

These changes have taken place in governments as well as in businesses. For example, modern digital systems have made it possible to overlay information related to geographic location in a manner which makes urban planning much more efficient. The information revolution and networked computing have made it easier to collect and analyze information relating to consumers' interactions with businesses. Developments in data processing allow business to use personal data to perform market research and tailor products and services to suit customers' preferences. These technologies can also be applied to companies' internal processes, for example, to data related to employees. Increasingly, businesses rely on their ability to transfer personal data from one country to another to achieve the best results in efficiency and customer service.

Much foreign direct investment is focused on services activities,¹ such as out-sourcing of customer service, and many countries are positioning themselves higher up the chain to more 'value-added' services output. The ability of countries to attract investment and nurture indigenous businesses will depend on them enabling the cross-border data flows on which the information economy depends.

¹ OECD Information Technology Outlook; ICTs and the Information Economy, 2002

BENEFITS OF FLEXIBLE PRIVACY PROTECTION

Information creates value when used by an organization to more accurately target the products and services it provides to match consumers' specific interests and needs. Those interests are predicted by analysis of the data collected from the consumer, data generated by the relationship, and information from others that have had a relationship with the consumer. This personalization has been expanded with the Internet and is another positive benefit of the information age. In the same way as local shop owners made it their business to know their customers and meet their needs, today, the most successful companies use sophisticated data collection and analysis systems to ensure they best serve their customers' wishes.

Digital technologies and the digital processing of information have brought benefits directly to consumers. Robust data flows have allowed business to:

- identify and meet individual needs;
- increase efficiency and lower prices;
- enhance consumer convenience;
- inform customers of new opportunities;
- expand access to services and products;
- detect and prevent fraud and other crimes²; and
- respond to demand shifts more quickly.

Concrete examples of the benefits to consumers of information processing and sharing include the following:

- In the United States, it has been estimated that the use of personal information by lenders has reduced interest rates by two full percentage points, saving consumers \$130-billion in interest charges every single year³.

² Putting People First: Consumer Benefits of Information-Sharing, Cate & Staten, 2000

³ Tower Group study, 1998

- The collection of consumer credit information by credit agencies has led to lending decisions being based on more objective and reliable models than previously. Studies have shown that this has resulted in the extension of credit to credit-worthy individuals who would not have been considered eligible under the previous system. This improvement has been made possible by robust information flows, and it benefits consumers, financial institutions and business.

However, the benefits of allowing the processing of personal data by business to create benefits for consumers go beyond simple financial gains. Companies also use customer data to help develop new products and services, creating an enhanced environment for entrepreneurship, and increased innovation which benefits the economy as a whole.

FUNCTIONS OF PRIVACY PROTECTION

There are four basic functions related to privacy protection that all jurisdictions should consider when drafting their approach to privacy protection:

- **Identification**

Identification includes analyzing technological trends, isolating threats to consumers, and suggesting how consumers might be protected from those harms. This can be done by businesses themselves, central authorities, regulatory agencies within their scope of responsibilities, legislative committees and academic research centres.

- **Education**

Consumers need to be educated about the uses of information, benefits those uses create, risks, and consumer rights and responsibilities. This education is the responsibility of government, business, consumer organizations, non-governmental organizations and even the media.

- **Implementation**

Implementation of privacy protection principles can be done directly, through legislation on either a sectoral or omnibus basis, as appropriate, and ensuring maximum clarity and flexibility, or through self-regulation, use of appropriate technology or other 'bottom up' processes including sectoral and/or company codes of conduct, corporate rules and individual customer empowerment.

- **Enforcement**

There are numerous ways to ensure that privacy protections are enforced, for example, through self-regulatory initiatives, legislation, regulation, or other forms of third party oversight. The most important part of enforcement is not the type of organization, but that it promotes trust in the data protection regime.

These privacy protection functions can be accomplished in different ways and by different organizations. Governments and intergovernmental organizations should recognize the legitimacy of other approaches as long as the essential privacy protection functions are met. For example, an approach that is focused on equivalent outcomes of other data protection regimes, rather than their mechanisms of enforcement, is the best way to ensure the continued international flow of data transfers, investment, and global trade.

PRIVACY PRINCIPLES

ICC advocates a privacy protection regime that offers sufficient protection to citizens while allowing the economy to flourish and thrive. Governments, business and other groups should agree on a solid core of privacy principles and then enable business to meet these requirements in the myriad ways companies may evolve in a thriving, competitive economy. The best way to provide a base level of protection and to implement these principles directly into the day-to-day business functions of a company is by adopting the guiding principles for privacy, which draw on the OECD privacy guidelines⁴, outlined below:

Principles for the use of personal data

- **Lawful and fair collection**

The collection of personal data should be by lawful and fair means.

- **Data Quality**

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose specification**

The purposes for which personal data are collected should be specified, and data subjects should be notified where data is being collected directly if the data are to be used for other purposes.

⁴ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

- **Use limitation**

Subject to legal obligations to cooperate with law enforcement authorities, personal data should not be disclosed, made available or otherwise used for purposes other than those specified above, if this use is likely to cause harm to the data subject.

- **Security**

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Openness**

There should be a general policy of openness about developments, practices and policies with respect to personal data. Individuals should be able to easily access the privacy policies of any organization holding their personal data.

- **Right of access**

Individuals should have the right to correct any inaccurate data relating to him being held by an organization.

- **Accountability**

A data controller should be accountable for complying with measures which give effect to the principles stated above.

IMPLEMENTING PRIVACY PROTECTION

Any privacy regime should permit the maximum number of ways to facilitate legitimate data collection and transfers. Some practical and flexible ways to ensure these principles are put to work include:

■ Codes of conduct

Individual companies or industry sectors can develop and implement codes of conduct which implement privacy principles directly in every-day business functions. Codes of conduct can create internal company rules and procedures which are binding on employees. Codes of conduct can be much more detailed and give clearer guidance to companies than national legislation, and they can more adequately ensure privacy protection in circumstances or business processes which law-makers did not anticipate. Depending on the type of code, it can be enforced where necessary by regulators, ombudsmen, enforcement agencies, sectoral organizations or industry associations. Company rules can also be monitored and enforced by internal procedures subject to employee contract clauses.

The recent report by the European Commission on the implementation of the Data Protection Directive (95/46/EC)⁵ signals the way for approval by the European authorities of codes of conduct for use by companies doing business in, and out of, the European Union. Governments in general should provide clear and practical guidance for the application of corporate codes, without the need for cumbersome registration or notification procedures, and with a streamlined approval process.

⁵ First report on the implementation of the Data Protection Directive (95/46/EC), http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm

■ **Contracts**

Contracts can be used by companies to transfer personal data to other companies. Contract clauses can ensure that the company to which data is being transferred matches the privacy protections provided by the company transferring the data. This flexible method allows companies to share and trade data which is necessary for development, marketing and other purposes, while ensuring that data subjects enjoy the same level of protection if their data are transferred. The use of contracts can be particularly effective when transferring personal data to another country with a different type of privacy protection. ICC, with other business organizations, has developed model contract clauses for the transfer of personal data to third countries outside of the European Union. These will enable companies to perform the day to day data transfers essential for doing business.⁶

■ **Seal programmes**

Seal programmes already exist in many countries, and act as a mechanism for businesses to assure their customers that privacy protections are observed. A company may join a seal programme, implement its privacy principles and practices, and allow itself to be audited or monitored by the seal programme, and/or have the seal programme act as an investigator and enforcer in the event of a customer complaint. This allows the company to display a 'seal of approval' such as a logo on its website or other company materials. As seal programmes act primarily to give information to customers making choices in competitive marketplaces, there is no need for seal-specific legislation.

⁶ Standard Contractual Clauses for the Transfer of Personal Data from the EU to 3rd Countries (controller to controller transfers) http://www.iccwbo.org/home/menu_electronic_business.asp

■ **Individual empowerment**

Individuals have many options when it comes to working pro-actively to control their personal data. The market has been responsive to consumers' desire for greater control, and many software products now exist to allow e-commerce consumers to decide when and how to divulge their personal data. Non-governmental organizations, governments and business have worked together to develop systems that allow consumers to set preferences on their browsers, and have those preferences matched against a business' server automatically (the Platform for Privacy Preferences or "P3P")⁷.

⁷ <http://www.w3.org/P3P/>

OVERLY RESTRICTIVE PRIVACY PROTECTION

In some countries, omnibus privacy protection legislation has been passed which, though intended to protect consumers and enable data flows to continue, has had many adverse effects for business and consumers. These adverse effects include:

- The cost of compliance with onerous privacy protection obligations is high, and does not necessarily provide a tangible benefit to data subjects by way of a noticeable improvement to the protection of their privacy. In many cases the processes required to ensure compliance are technically unfeasible, particularly for businesses making comprehensive use of the Internet. These factors can affect investment decisions.
- Despite enormous effort and expenditure by business and governments to increase the level of data protection, consumer confidence has not been observably boosted. The benefits to consumers of many data protection requirements are unclear, and consumers are often unaware of the level of privacy protection they enjoy, with the result that consumers in countries with high levels of government regulated privacy protection are no more reassured than those in more flexible systems.⁸
- The development, introduction and marketing of new products is hampered. For example, a company wishing to gauge potential demand for a new product line may have difficulty in accessing sufficient and comprehensive customer data outside of its own customer database. Similarly, marketing a new product is hampered when obtaining comprehensive lists of potential customers is restricted.

⁸ IBM Multi-National Privacy survey, 1999

- Data restrictions on the collection and use of personal data by third parties particularly affect the development and growth of new companies and small and medium enterprises (SMEs). These companies do not generally have established databases of existing customer relationships to use in their research and marketing. Businesses such as these may rely on data collected and analyzed by other companies. However, the use of personal data by third parties is particularly targeted in countries with restrictive privacy protection regimes. This particularly reduces the ability of small and start-up companies to do essential research and marketing.
- Companies whose business involves transferring personal data to other countries with different types of privacy protection face difficulties as privacy protection legislation can forbid these transfers. This can also affect companies operating in the countries to which the data would be transferred. For example, many companies have taken advantage of improvements in the communications infrastructure and the availability of skilled workers in countries outside their main bases of operation to create customer service response centres, such as call centres. This allows companies to provide 24-hour customer service at a competitive price and creates employment around the world. However, for these call centres to operate effectively, they must have access to the customer data of individuals in another country. Restrictions on transferring personal data, or the imposition of onerous burdens on companies, which are disproportionate compared to the interest they are intended to protect, can result in less convenient and competitive customer service, and can also hamper job creation in emerging economies.
- Overly restrictive privacy protection regimes can result in companies choosing to locate their operations elsewhere. One example of this was the decision of US financial institutions to stay out of the European consumer lending business because restrictive privacy laws acted as a competition barrier.⁹ By reducing the information available to market

⁹ Summary of Tower Group Studies Related to Opt-In, 2001

entrants to develop and market new products, and by effectively imposing disproportionate compliance costs, overly restrictive privacy protection can raise the costs of market entry to a level at which companies will judge that investment is not worthwhile. These lost opportunities affect not only employment figures, but also the overall competitiveness of the market and countries' economies as a whole.

Restrictive privacy protection regimes harm the introduction of new products, services, and delivery channels, and the growth and development of new companies and SMEs, effectively creating barriers to market entry. They also create significant problems for companies engaged in trans-border data flows, the very companies which many countries wish to attract for the purposes of foreign direct investment.

ACTION ITEMS FOR GOVERNMENTS

Governments should further recognize that the Internet is a medium providing new opportunities and challenges. Heavy-handed privacy laws and regulations can have the unintended consequence of stifling innovation and growth. Data protection and privacy regimes need to be flexible enough to keep up with changing societal needs, new technologies and innovation in business methods. Existing regulatory systems must, of course, provide consumers with useful protection of their personal data, but at the same time must guarantee the free flow of information needed for the information society to produce the anticipated benefits. Governments should also recognize that government regulation or 'top down' legislation may not be the most effective way to achieve an acceptable level of privacy protection.

ICC encourages governments to take the following steps to achieve optimum privacy protection:

- Adopt principles to ensure adequate data protection, such as those included in this document, and in doing so not exceed the principles set forth in the 1980 OECD Guidelines.
- Adopt a flexible and responsive approach to the protection of personal information, including the acceptance of self-regulatory solutions and technological innovations that empower the user, determining where specific laws are needed to protect consumers from harm and enact those laws in the most targeted fashion possible.
- Educate the public about privacy protection and the use of privacy-enhancing technologies.

- Cooperate internationally to ensure a seamless environment for different privacy regimes. In assessing the level of protection provided to personal information in other jurisdictions, the criterion should be the objective level of protection afforded by the system as actually used in practice within that jurisdiction.
- Governments should avoid developing laws, policies and practices that create obstacles to transborder flows of personal data.
- Endorse model contracts, codes of conduct, seal programmes, and other self-regulatory mechanisms prepared by the private sector in order to promote the free and secure flow of information within and between companies, and across borders.

