Manager's Guide to

Data Privacy

Discreet Use of Personal Information

by Bob Blakley, Jacques Remi Francoeur,
Steven Jenkins, Eliot Solomon,
and The Open Group Security Forum

THE Open GROUP

Manager's Guide

Data Privacy
Discreet Use of Personal Information

ISBN: 1-931624-33-X

Document No.: G033

Published by The Open Group, July 2003.

Any comments relating to the material contained in this document may be submitted to:

ogpubs@opengroup.org

contents

This Guide – is it for you?

You have heard a lot about the issues of privacy and information systems in recent months. You may have heard of cases where companies misused private information. You're aware that public policy issues have been raised about how governments and law enforcement agencies might be given access to information about individuals, and about the responsibilities of private organizations to cooperate. Perhaps your industry has canons of ethics concerning the privacy of your clients.

And you may be wondering what it all means for you. Your business is more and more dependent on computers and information technology. If you're like most businesses, you are keeping more of your business information as data in computer systems. And if you are taking full advantage of what computers can do for your business, you probably have more information about your employees and customers at your fingertips than you ever did before. And there are more ways for you to get, share, and exploit the information you have than ever before.

As a business manager who conducts an efficient and profitable business you want to know exactly what you must do to meet the requirements of law and the regulations that affect you. As an ethical and responsible business leader, you want to be sure your business is conducted in a way that always respects the rights and expectations of your customers and employees. And, as a mere mortal, you are probably uncertain what all the things you've heard or been told really mean. You've gotten conflicting advice from different sources, and you are concerned that you may be looking down a bottomless pit of additional IT expenses.

If this in any way sounds familiar, then this Guide is for you.

About The Open Group

The Open Group, a vendor-neutral and technology-neutral consortium, has a vision of Boundaryless Information Flow achieved through global interoperability in a secure, reliable, and timely manner. The Open Group mission is to drive the creation of Boundaryless Information Flow by:

- ❑ Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- ❑ Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate open specifications and open source technologies
- ❑ Offering a comprehensive set of services to enhance the operational efficiency of consortia
- ❑ Developing and operating the industry's premier certification service and encouraging procurement of certified products

The Open Group provides opportunities to exchange information and shape the future of IT. The Open Group members include some of the largest and most influential organizations in the world. The flexible structure of The Open Group membership allows for almost any organization, no matter what size, to join and have a voice in shaping the future of the IT world.

More information is available on The Open Group web site at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes White Papers, Technical Studies, and Business Titles. Full details and a catalog are available at www.opengroup.org/publications.

Trademarks

Acknowledgements

The Open Group gratefully acknowledges the initiatives from Bob Blakley and Jacques Francoeur in setting out the essential content of this Guide, and the valuable additions and editing by Eliot Solomon and Steven Jenkins in leading The Security Forum to produce this balanced presentation on this important subject.

Chapter 1

Why Privacy Matters to your Business

Simply put, privacy matters to your business because it matters to your customers, suppliers, and employees. Let’s look at some of the ways this is so.

When you seek treatment for a medical condition you probably don't want the world to know. What books you read or movies you watch is your business, and not your neighbors' or the government's. Your family’s financial details shouldn't be public knowledge, but a matter of confidence between you and your bank. (And what balances you keep at one bank are no business of other banks where you keep accounts.) Parents of children receiving treatment for learning disabilities want to protect their children from prejudice.

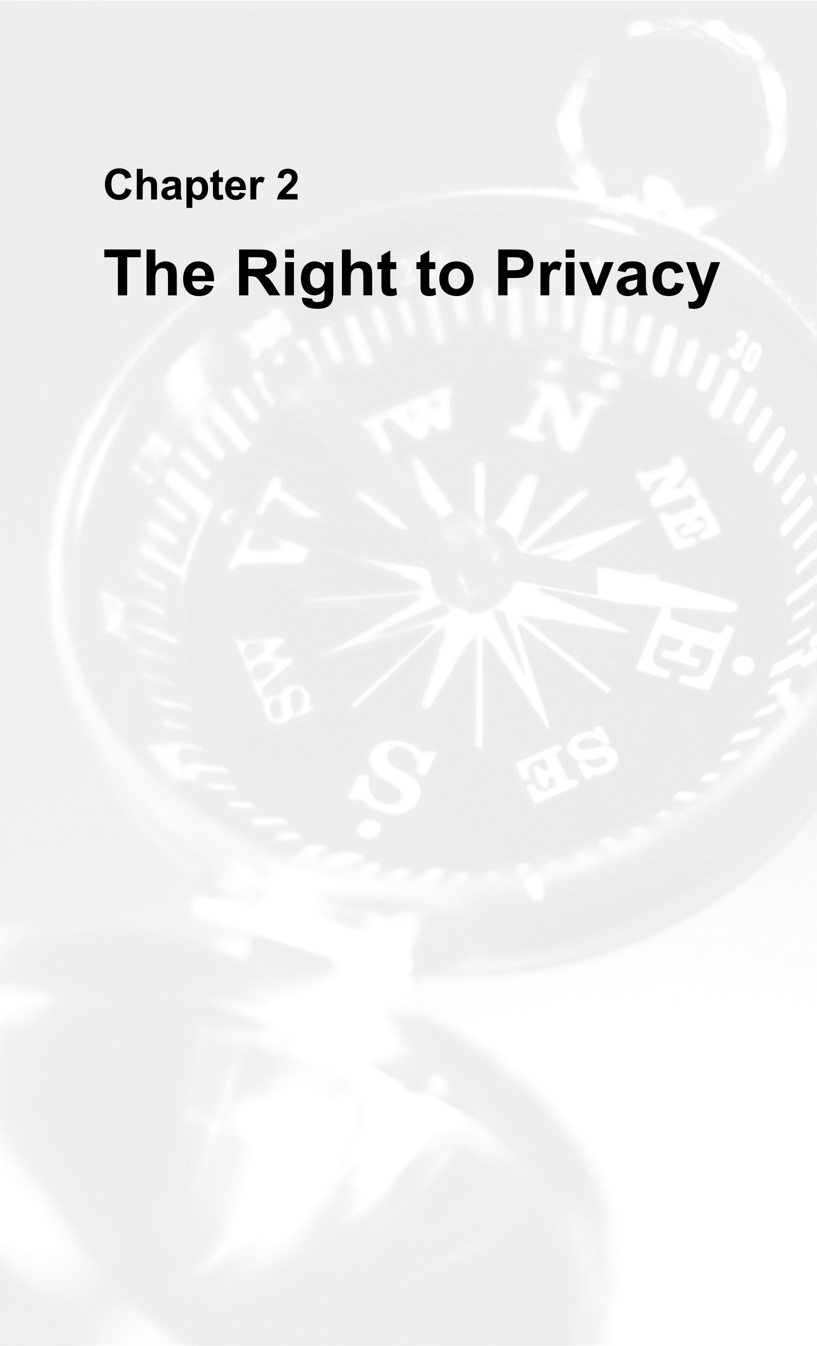
People who are concerned about privacy don’t necessarily have something to hide. All of us have details that we’d prefer to keep private: love letters, family photographs, financial history, to name a few. The point is that people care about their privacy, and it really doesn’t matter why. They do, and that’s the world you have to do business in. If privacy were the only concern of customers, it would be simple to safeguard it. All business would be conducted anonymously, in cash. If no personal information is disclosed in a transaction, there’s nothing to protect. Unfortunately, it’s not that simple. Doing business requires customers and suppliers to know some things about each other.

For example, you expect your healthcare provider to know your medical history in order to, among other things, avoid prescribing a drug that you’re allergic to. You expect your rental car company to know your preferences, and perhaps your credit card numbers. You expect your employer to know your salary, and perhaps your checking account number so that he can deposit your salary directly (but not so that he can see how much money you have). Likewise, your customers may expect you to remember them and to tailor your service to their needs and likes. Protecting the privacy of your customers and suppliers is important whether you use computers or not. Respecting your customers and their privacy is not a property of technology – it's a way of doing business. If you *are* keeping computer databases or conducting eCommerce over the Internet, however, you have a greatly enhanced ability to collect personal information, and greater opportunities to divulge it inadvertently. Electronic information can be copied and exchanged easily and quickly, and unauthorized copies may be impossible to undo.

The privacy of your employees is just as important as that of your customers and suppliers. An employer often needs to know highly personal information about its employees in order to withhold taxes properly, provide medical and/or insurance benefits, offer assistance programs for substance abuse or other personal problems, or plan career growth. Every employee expects his employer to protect his privacy. Consequently, good privacy protection policies and practices are a prerequisite for hiring and retaining quality employees.

Chapter 2

The Right to Privacy



People often discuss a “right to privacy”. Many people believe that the right to privacy is a self-evident, inalienable human right. In some countries, the right to privacy is considered a constitutional right, one that cannot be violated by the government. Even in countries where there is no constitutional basis for a right to privacy, laws and regulations provide individuals with assurances that their privacy will not be violated.

These laws and regulations often protect privacy from violation not only by the government, but also by companies and other individuals. At a minimum, such laws provide penalties for violating someone’s privacy. In many cases they create affirmative obligations to protect privacy.

Often, the rights given by law and government regulation are further extended by private bodies and associations. The canons of ethics for lawyers and the oaths taken by doctors are examples of privately undertaken protections of individuals’ rights to privacy. We’ll discuss some of these formal protections of privacy later in this Guide.

Respect for privacy, however, is not primarily a legal obligation. Even in areas where privacy is not protected by formal structures, social custom and the principles of respect for others give people an expectation that their privacy will be respected. Legislative safeguards for privacy are the *consequence* of widespread belief in privacy as a fundamental human right, not the cause of it.

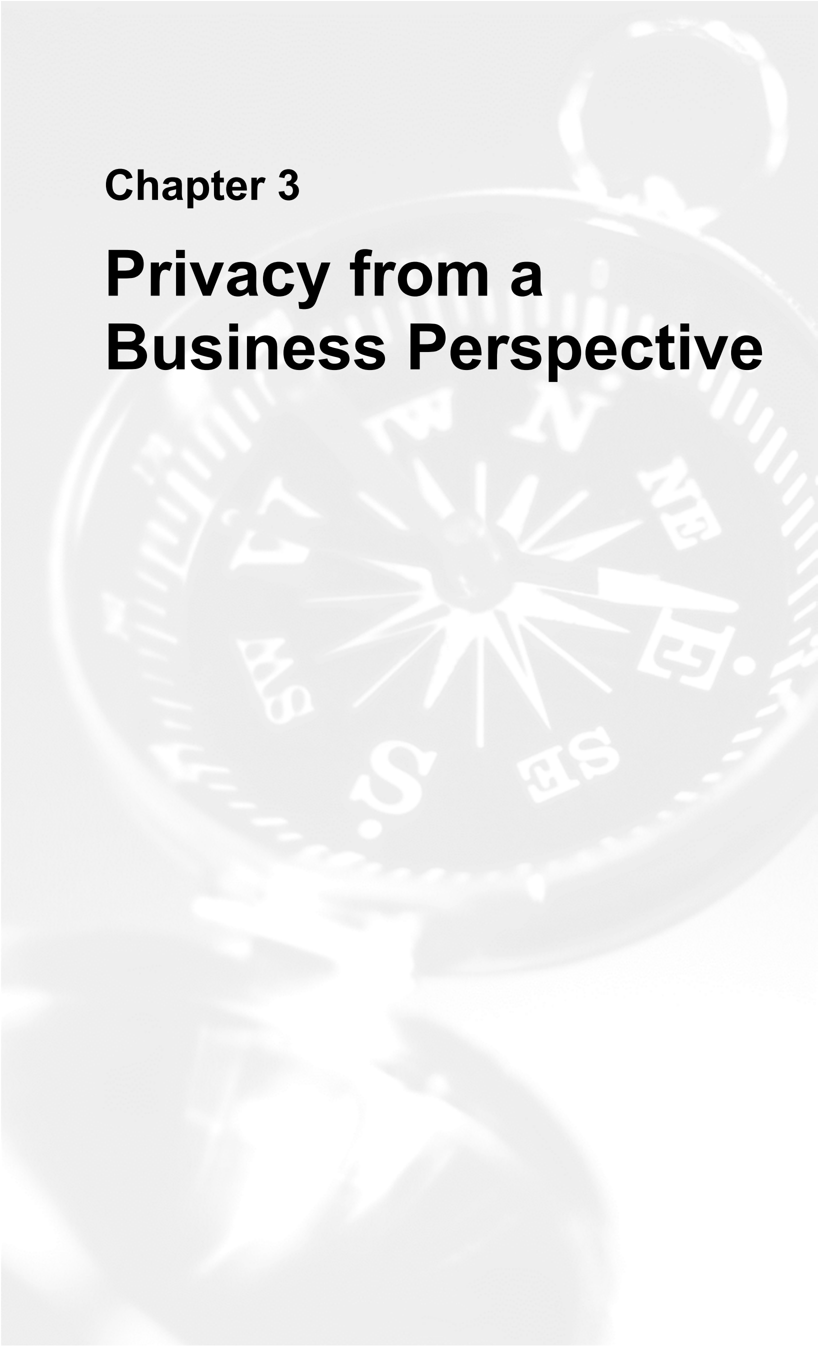
As the world grows smaller and more interconnected through information technology, reliance on goodwill and social contracts needs additional support. Governments and other organizations all over the world have been enacting strong measures to protect personal information from unauthorized collection and disclosure. Following are some examples.

The European Union (EU) adopted a Data Protection Directive in 1998. This directive has now been written into law in almost all EU member countries. Other EU directives also address the issue of privacy. In the United States, sector-by-sector regulations have been adopted to protect the privacy of personal financial information (the Gramm-Leach-Bliley Act), personal medical information (the HIPAA Privacy Regulation), educational records (the FERPA Regulation), and personal information about minor children (the COPPA Act). Canada adopted a comprehensive national law (the PIPEDA Act) in 1998 to protect the privacy of personal information.

Legal requirements for privacy protection vary by locale. You will probably want to consult with your lawyers on privacy issues, in exactly the same way that you consult with them to shape your business practices for hiring and firing, labor relations, taxation, etc. But these are details. And simply meeting the law’s minimum requirements is not the objective. The important point is that respect for privacy is important to you as a business person because it is important to the people who matter to your business: your customers, suppliers, and employees.

Chapter 3

Privacy from a Business Perspective



Respect for privacy

Respect for your customer and his privacy is one of many intangibles that matter in business. Integrity, dignity, diligence, and competence are others. And like those others, respect for privacy does not apply itself. Nor can you just buy it and install it. Making your respect for privacy an effective business advantage requires you to understand how your customers value that respect, and what they would see as a violation of their trust.

You then have to set your business objectives and adapt your practices to take advantage of the goodwill your respect for privacy creates. This goodwill is a “renewable resource”, but one that can be rendered worthless if you give offense to your clients’ sense of their own privacy. But managing intangible assets and creating customer loyalty are the sort of informed business judgments that you make every day as a manager.

Let’s look a little closer at some of the business impacts of respecting, and failing to respect, privacy.

Reputation, loyalty, and market share

As we’ve noted, consumers are concerned about their privacy. If your customers develop confidence that your business uses personal information in a straightforward and responsible manner, they may be reluctant to switch to a competitor whose privacy practices are unknown.

EarthLink features privacy issues prominently in its marketing strategy, including high-profile television commercials with amusing but pointed vignettes illustrating privacy violations. Attention to privacy concerns can be positioned as a competitive advantage.

On the minus side, the public sensitivity to privacy issues is so high that mis-steps can lead to public backlash and lasting damage to your hard-won reputation.

In 2000, Doubleclick, Inc. was embroiled in a firestorm of negative publicity when consumers and privacy advocates learned that it planned to combine information on some 100 million web surfing "profiles" with personal information like name and address. In 2002, Doubleclick settled a number of lawsuits that followed the revelations, and agreed in the settlement to modifications and an independent audit of its privacy practices.

Comcast Corporation is currently the target of a class action lawsuit alleging that it violated the privacy of its one million users by collecting information on their web surfing habits.

Eli Lilly recently apologized in public for an event in which the email addresses of users of its antidepressant drug Prozac were revealed in a mass emailing.

It's worth noting that in the age of the Internet, the public's memory for scandal is much longer than it used to be. A potential customer with a hazy memory of some event involving your company only has to type a few words into a search engine to find all the gory details, preserved for perhaps years on a web site.

Risk, profit, and the bottom line

As a manager, you already know that things that adversely affect your company's reputation affect your bottom line. There are other ways that privacy matters to both sides of the balance sheet.

If your privacy policies and practices are sound, then you can collect the kinds of information from your customers that helps you be a better supplier. In more heavily regulated markets (e.g., products for young children, healthcare), good privacy practices are the cost of admission—you simply can’t stay in business there without them.

Even if they don’t lead to scandal, failures to protect privacy may cost you money. The most direct way is that you might have to terminate certain business operations because they violate your policy, your customers’ expectations, or the law. Best Buy Co. disabled its wireless cash registers for a month in 2002 over concerns about transmitting customer information in the clear (that is, unencrypted). Could there be a more apt example for lost revenue than turning off the cash register?

Privacy violations can also cost your company money in a less direct but perhaps far more drastic way: civil and criminal penalties. Toy manufacturer Lisa Frank was fined $30,000 by the U.S. Federal Trade Commission for violation of the Children’s Online Privacy Protection Act. The EU Privacy Directive provides for, among other things, compensation for individuals whose privacy is violated.

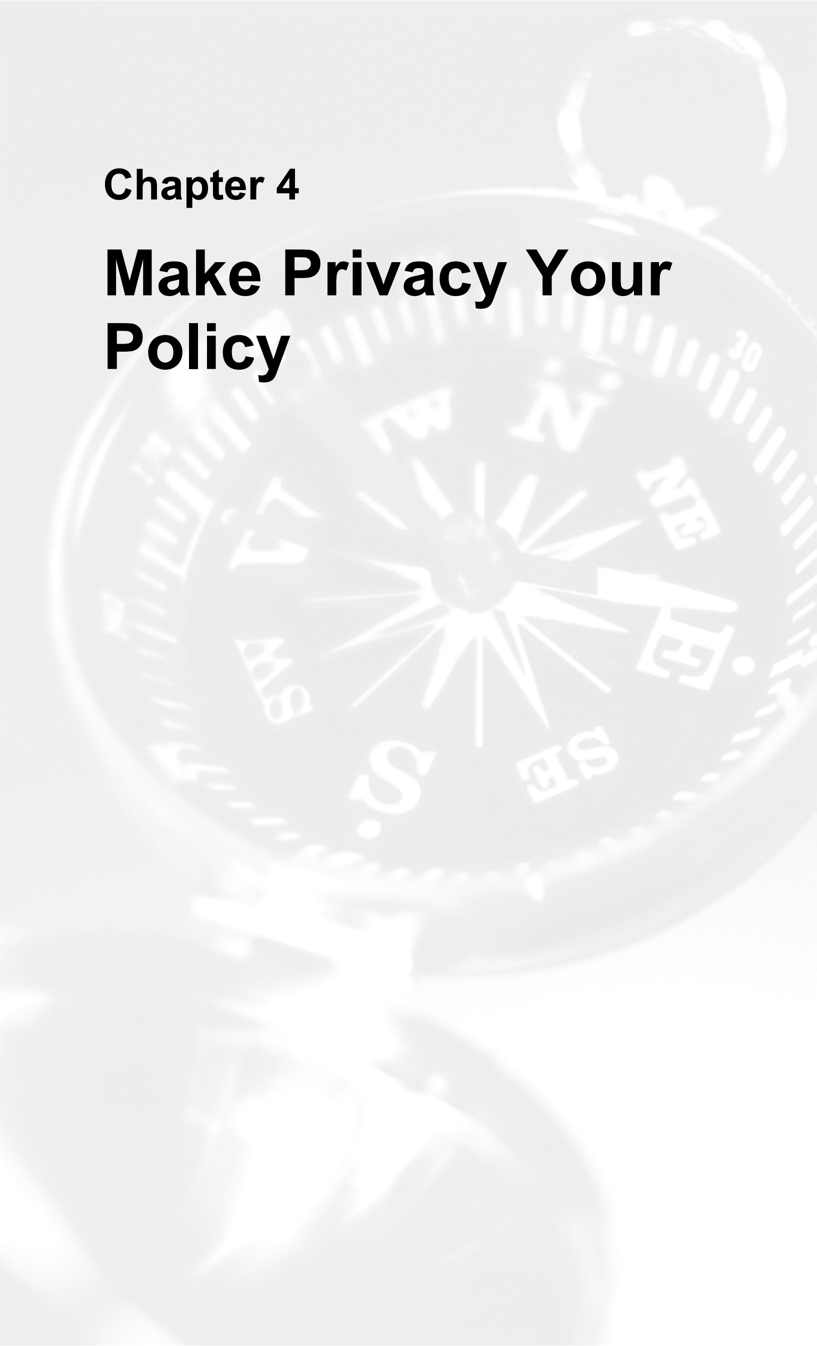
Costing your company money is a bad thing, but there are even worse things that can happen to you if you abuse privacy. You can go to jail. For example, the U.S. Health Information Portability and Accountability Act provides for criminal penalties for unauthorized disclosure of personal information.

The bottom line is, well, the bottom line. Failing to respect the privacy of others can cost your company money—or worse.

Privacy in particular, and information security in general, are often perceived as burdens that interfere with “real work”. And that's true if your respect for your customer is an afterthought. But if you make your concern for your customer a fundamental part of the way you do business, privacy protection and information security are integral parts of your “real work”. They enhance your product or service by making it more reliable, more trustworthy—in short, more valuable.

Chapter 4

Make Privacy Your Policy



At the center of every corporation is a set of goals and values that drive its operations. Policies keep all the parts of the organization pulling together toward the goals. Whether they are written out in a corporate manual, or informally shared as “the way we do business”, your business policies describe how you work, and how your business deals with others. They tell who can and should do what, and under what conditions.

For instance, the information you keep about employees is governed by your HR policies. You probably have an HR Policy Manual to ensure that you comply with government regulations and your obligations to your various benefits programs. Policies also tell your people what they can’t or shouldn’t do. For example, you almost certainly have policies against taking company documents out of the offices.

In the Manager’s Guide to Information Security[1] we explained how corporate policies should guide what you want security systems to do. We give the same advice about systems to help you maintain privacy. A privacy solution will be designed to help you enforce company policies about the collection and use of information about customers, partners, employees, and others. A good privacy solution will help prevent misuse of information in your computer and IT systems. A better privacy solution will help you conduct your business in a way that is always respectful of the rights of others.

A privacy solution that requires you to change the way you do your business to meet *its* notion of appropriate policies is not one you should use. You decide what policies your company should follow and, if they're right for you, your privacy solutions and systems should conform to them.

[1] Manager’s Guide to Information Security, Doc. No. G250, published by The Open Group.

How do you use corporate policy to guide your privacy solutions? First you have to do your part. Make sure you really know your policies, and why they are right for your business. Review them periodically to be sure they still meet both your needs and the expectations of the people whose privacy you need to protect. Remember, business and the competitive environment change. And these days, people's expectations about privacy and computer-based services are also changing. Your policies will have to change over time as well.

Be sure everyone in your company knows what your *current* policies are. Tell the people helping to create your privacy solutions that you have policies, that you know why they are right for you, and that you want them to be included in the design of the privacy solution. And make sure that, as you change and evolve your policies, you will be able to update your privacy solutions to match your policies.

You may not have given specific consideration to the way your company policies address privacy, but you've probably made your policies with respect for customers and employees in mind. It probably won't be difficult for you to identify the policies that relate to privacy, and from them create your company's privacy policy. To get you starting to think about your privacy policies, we offer the following suggestions about what your policies should include.

Limit collection

The consent of subjects to collect and retain personal information for a purpose needs to be specific and explicit. Having permission to collect one piece of information for one purpose does not entitle you to collect other information for that purpose.

Clearly, this issue involves human judgment. No technical solution alone can ensure that your data collection is consistent with a policy of limitation of purpose. The technical solution can, however, maintain a permanent association between the collection processes and the appropriate consents. The association itself will not do anything, but it will make it easier for you as a business manager to ensure that the two are in sync.

Give notice

When you collect personally identifiable information, it’s important to say why you’re collecting it and how you plan to use it. In addition to any legal requirements there might be for notification, being clear about your purpose may help to improve the quality of the information. Look for solutions that make it easy to give notice, and remember what the notice was. If you can associate the notice with the information, then you’ll have a reliable means of deciding whether some future use of the information is allowed.

Get consent

It’s not enough merely to give notice—you need to get permission. Before you collect, disclose, or use personal information, you need to have the informed and unambiguous consent of the subject of the information. The notice we discussed in the previous section is part of the process. Other steps require ensuring that the subject person sees and reads the notice (or hears it read), and affirmatively agrees to it. And as with notice, look for the ability to remember the agreement and associate it with the information. Remember that some personal information might be kept in your files for a long time (for example, employee records). You will need to keep the consent as long as you keep the information.

Limit use

Similarly, your privacy solutions need to maintain a permanent association between data uses and consents. You'll need the ability to review potential new uses of personal information to ensure that they're consistent with the consent.

You've probably noticed the recurring theme by now: the things to look for are the things that help you ensure that your company's policies are being followed, that the subject of the information has consented to its use, and that deviations from your policies are discovered.

Limit retention

If your business keeps personal information longer than you need it for the agreed purpose, you may be incurring unnecessary risks. For example, old information may be out-of-date. If you make business decisions on the basis of wrong information, you may make wrong decisions. If you disclose wrong information, you may incur liability.

Of course, destroying old information doesn't ensure that current information is correct, but it does prevent the mistake of confusing old and current information.

Your privacy solutions, therefore, need to provide you with simple ways of dating information – not just the date it was collected, but also the dates of any corrections or additions.

It might have occurred to you by now that there's nothing unique about privacy in that regard. Well, you're right. All business information, whether personal or not, needs to have a legacy or provenance associated with it: where it came from, how trustworthy it is, who is responsible for it, etc. Technology solutions for all kinds of business information problems need to support keeping up with the provenance of that information. Privacy of personal information is just an example, but one that you should probably pay special attention to.

Get it right

All business information needs to be accurate, but personal information is especially sensitive. To labor the point, personal information is information about real people, and it matters to them if it's wrong. You, as a business person, have a duty of care to ensure that information you collect about people is accurate for the agreed purpose. The technical solutions you deploy need to make it easy for you to subject your personal information to reviews and audits.

Keep it discreet

Clearly, one of the most important things you can do with personal information is to ensure that it is never disclosed inadvertently. Unauthorized disclosure is clearly one of the greatest concerns of individuals. They want to be assured that their information is never given to people who shouldn't see it – or worse – published.

Know who's accountable

Another thing you need to look for in privacy solutions is the ability to know who controls what information. Your business is accountable for personal information in its control. It's important to note that controlling information is not the same as merely storing or using it. Control has to do with deciding what the information is, not just where it is or who can see it.

In many organizations, a specific person is assigned the responsibility for controlling personally identifiable information. It's not necessary at all to have a special position like "Chief Privacy Officer", but someone should be in charge. Look for the ability to clearly name such a person in your privacy solutions. Of course, the solutions also need to give the named person the *ability* to actually control information, not merely the responsibility.

Be forthcoming

Your policies regarding collecting, processing, and disclosing personal information should be communicated, at least to those about whom the information pertains. You may find that it's best to publish those policies. Published policies give individuals confidence that they are getting equal treatment.

Look for privacy solutions that make it easy to be forthcoming about your policies. Whether it's by letter, contract, web page, or other means, informing users of your personal information policies should be a seamless, integrated part of doing routine business.

Co-operate

People are clearly concerned about the uses of their personal information. One way to ease their concerns is to allow them to see any personal information you keep about them. An even better way is to ensure that people have the right to review their personal information and to request revisions or corrections. In addition to increasing the confidence of your customers, suppliers, and employees, you may find that opening your information up for individual review increases the accuracy, and therefore the business value, of that information.

Giving people the ability to review and amend their personal information need not require a high-tech online system. It can be as simple as the ability to print form letters and correction forms. Whatever form it takes, be sure to look for this feature in privacy solutions you select.

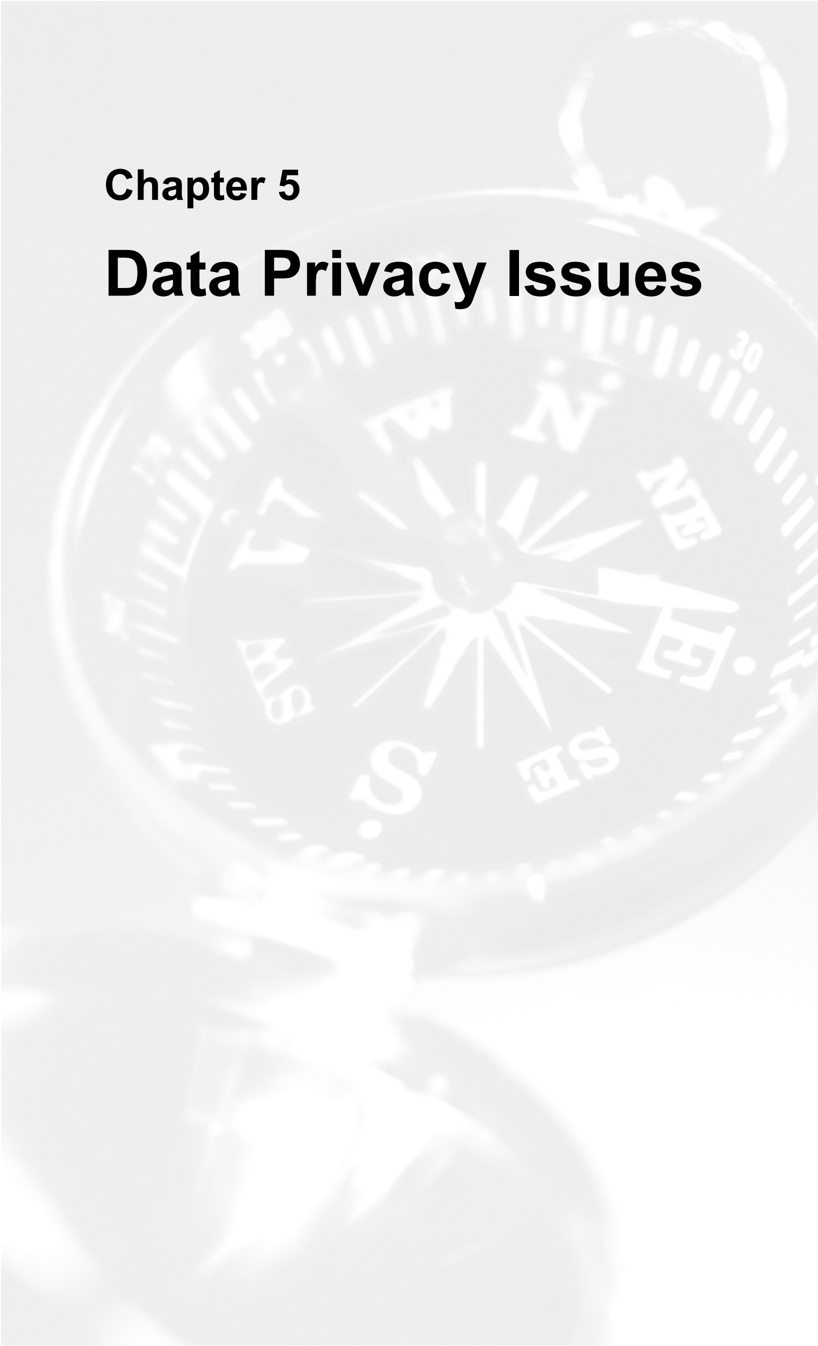
Listen

If you collect personal information, you have the ability to change people’s lives. They will probably have opinions on how you do it, and how you ought to do it better. If you’re not complying with the law, or if your corporate policies are not always followed, someone is likely to complain about it. Even if you comply with the law and your policies, someone may suggest things you can do better.

You should designate a person to listen to and act on all complaints and suggestions regarding privacy. Your solutions need to make it easy for people to reach the designated contact. Doing so can be as simple as including a phone number or email address on every document that deals with personal information.

Chapter 5

Data Privacy Issues



Technologists, legislators, regulators, and lawyers have highlighted specific issues and objectives for privacy in general, and privacy on the Internet and in computer-driven businesses in particular. The rest of this Guide will focus on the specific issue of “data privacy”, which is a part of computer privacy. Before we focus on that, it’s worth discussing some other aspects of computer privacy.

Three cautionary examples

Your computer systems and the Internet give you the ability to reach out to your customers, employees, and others in powerful ways. As you do that, you might, without meaning to, intrude in areas the other person may consider private. One example is “spam”, the email equivalent of a telemarketer’s dinner-time phone call. Some people get so much unsolicited email – some of it patently offensive – that they have been moved to seek legislative protection against it. If you add to this burden of unsolicited commercial email you will be seen as a company that has no respect for privacy. Once that happens, your efforts to respect “data privacy” may satisfy your legal obligations, but it won’t gain you any useful goodwill. So exercise discretion when you send email. Consider the message you send, and to whom you send it. Whether you’ve collected email addresses or bought or rented a mailing list, be sure the addresses were collected from people who are going to be pleased to hear from you.

Collecting and using information about people’s activities may not violate the rules of data privacy if the information is made anonymous. That is, if you record that *someone* purchased such-and-such merchandise from you in a single day, but don’t record *who* that person was, the information you collect will probably not be subject to data privacy regulations. Collection of such demographic information is, of course, a useful business tool. Remember, though, that demographic groups are made up of private individuals. Increasingly powerful data analysis tools allow demographic data to be refined to a point where the difference between the public group and the private individual is small, and its use may give offense. When you use “anonymous” information be sure to remember the principle of respect for the individual’s sense of privacy.

To improve the “experience” of a web site, it is common practice to send programs to run on the computer of the person visiting the site. Some of these programs are called “scripts” and “applettes”. More powerful programs are sometimes called “plug-ins”. There are other ways to download programs to the site visitor’s computer, including as attachments to email. Sending such programs to other people’s computers is a legitimate way to improve the service your company provides. But remember that any program you send to someone else’s computer represents your entry into private space. It makes you a guest in the other person’s home, and obligates you to behave as such. Clearly, programs that gather private information and send it back to you without permission are a violation of privacy. But *any* excessive or unwanted use of your host’s computer would be an abuse of his hospitality. As with commercial email, be sure your program is delivered only to people who are going to be pleased to welcome the visitor, and be sure not to overstay your welcome.

These three examples all illustrate the basic principle of privacy: show respect for the other person. If you, through your IT capabilities, do not consistently show respect, your efforts at data privacy will always be suspect, and earn you no goodwill.

What is data privacy?

One definition of data privacy is “the protection of personally identifiable information”. This is an important definition, and is the basis for many of the laws and regulations concerning data privacy. But we consider data privacy to be somewhat broader.

As we discussed in the cautionary examples, many people may feel their privacy has been violated in ways other than just a failure to protect information about them. We would add to "protection of personally identifiable information" these other elements of privacy. First, we include the assurance that computer systems or the things they create or make possible will not intrude into one's home or life. Second, we include the principle that information stored "anonymously" as demographic information or about third parties should never be used in ways that feel intrusive. Information about fathers ought not be visited on their sons.

Personally identifiable information

"Personally identifiable" is a legal or regulatory notion that applies to certain information. In general, information is considered personally identifiable if it can be linked, directly or indirectly, to an individual person.

For example, names, addresses, Social Security numbers, driver's license numbers, etc., are all ways of identifying a person and therefore personally identifiable. Any additional information you associate with such data (say, your customers' shoe size, or music preference) is also personally identifiable, because it can now be linked to a person.

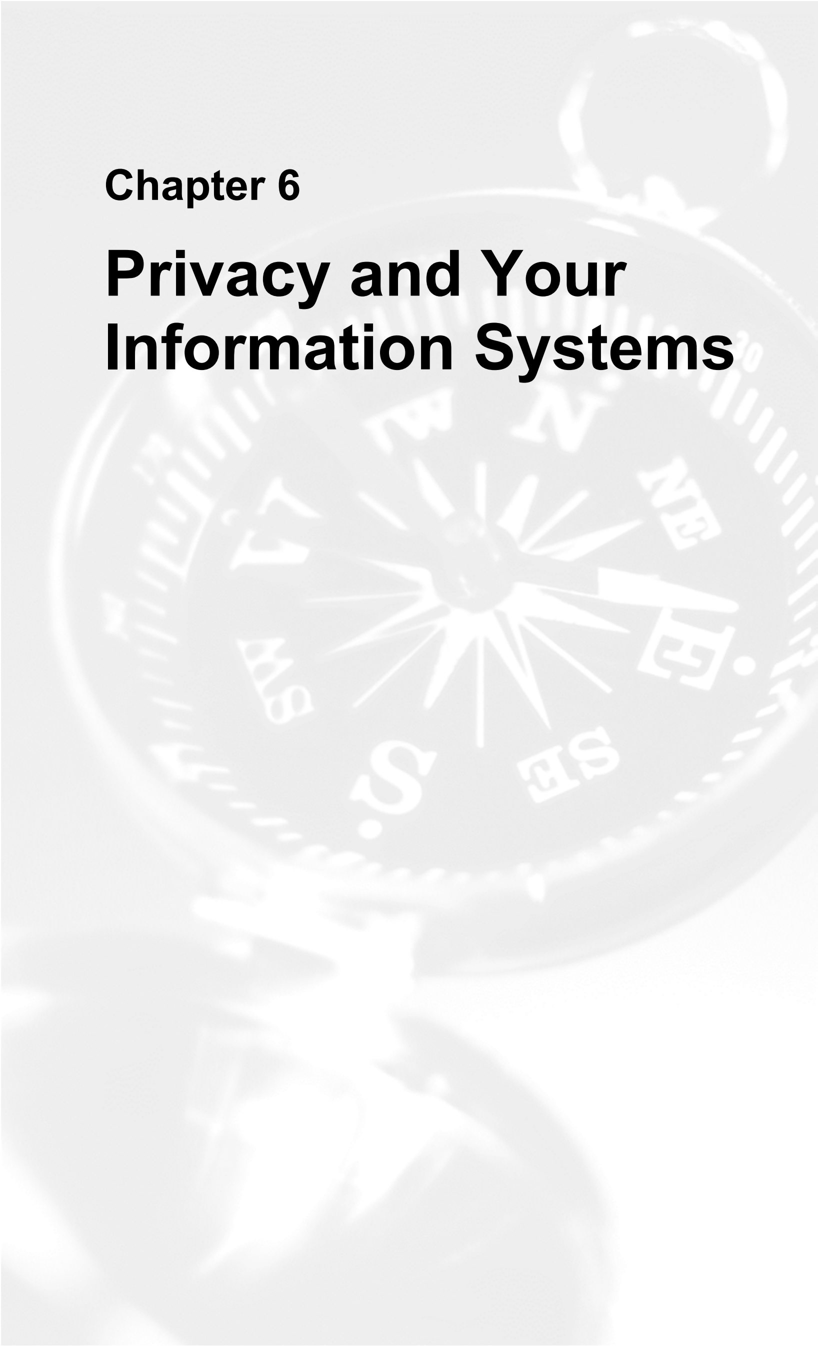
In contrast, summary or statistical information about a group is not generally considered personally identifiable. A table showing the genre preferences of all movie renters in a certain zip code is not personally identifiable information. Balance sheets and other summary business information are not personally identifiable, in general. Note, however, the use of "directly or indirectly" in the definition. If it's possible to parse or refine statistical data down to the individual person, the information is personally identifiable.

Information need not be stored in a computer to be subject to data protection laws and regulations. In some jurisdictions, the same protections apply to paper records, video recordings, etc.

Also remember that you may be keeping personally identifiable information about your employees, associates, or others in addition to your customers. Be sure to treat them with the proper discretion as well.

Chapter 6

Privacy and Your Information Systems



We hope we've made it clear by now that privacy is not a "computer" concept. It should be just as clear that computers and information systems can threaten privacy protection. In this section, we'll talk a little about how information systems can help you *protect* privacy.

Many information technologies contain the low-level mechanisms you need to protect privacy. Relational databases, for example, generally have some form of "logging in" and often give you the technical means to control access to data on the basis of rules. Every technology, unfortunately, does it a little (or maybe a lot) differently. So we can't give you *specific* advice on precisely *how* to protect *your* information and systems. We *can* give you some general advice on technology categories that may help you achieve your privacy protection objectives.

Technologies that promote data privacy

Information technology vendors will offer a variety of products which claim to help you protect privacy. You'll need to evaluate these claims and decide whether what's being offered is useful to you. Generally, technologies will help you to protect privacy if they do one of three things: 1. Identify which information is private, 2. State and enforce rules for the use of private information, and 3. Record what has been done with private information and produce reports.

Information Labeling

Information labeling is a venerable technique that isn't discussed much nowadays but is nonetheless very useful. An information label simply describes attributes of the information it's attached to. Applications read the information label to know what can and cannot be done with the information.

Information labeling helps you to identify privacy-sensitive information; it’s useful when you need to remember whether a piece of data has a particular property. If you label all the private data in your possession (for example, with labels like “personally identifiable information – address” or “personally identifiable information – medical”) then you’ll be less likely to forget that it’s personal information and use it improperly.

Security

Once you’ve figured out what private information your business is collecting and using, you need to regulate the use of private information by enforcing rules. Security technology (especially access control systems) will help you to do this. You’ll certainly need a way to know who wants to use the information and why it’s being requested. You may need to have ways for the requester to prove his identity, and ways to verify that he has been authorized. You’ll also need to keep records of what you’ve done with private information (so that you can respond to users’ inquiries, for example). Auditing systems can help you with that.

Workflow

An important factor in maintaining privacy is ensuring that sensitive information doesn’t get inadvertently sent to the wrong place. There is a class of information technology called *workflow* that gives managers the ability to translate their business processes more or less directly into computer implementation. Because workflow systems are rule-driven, they make it easier to ensure that technical processes follow the rules. And workflow systems usually come with powerful auditing capabilities, so they can help you with record-keeping.

The cost of protecting privacy

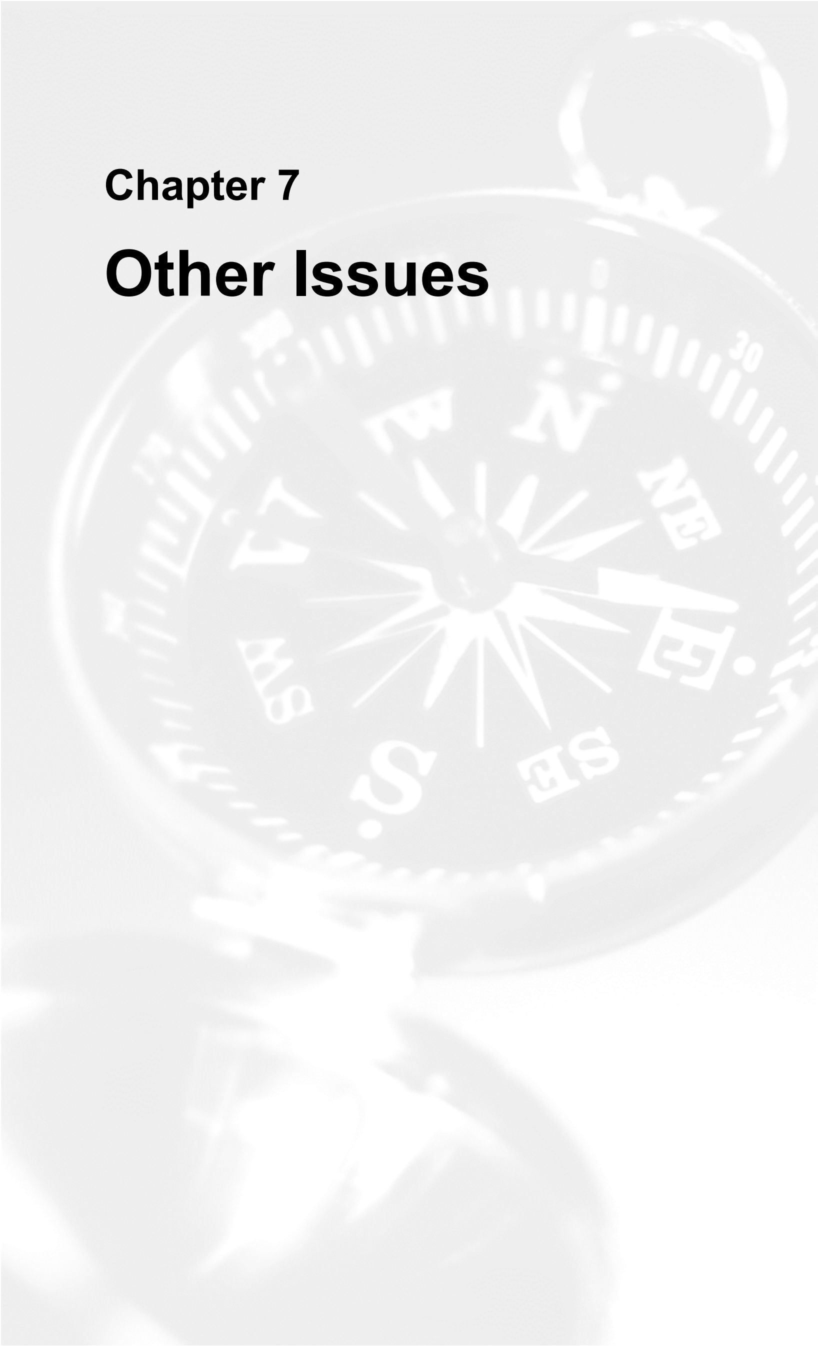
If you treat privacy compliance as a new activity, different from anything you are already doing, and you create a new organization to put together a compliance program from scratch, you'll probably spend a lot. But you don't have to approach privacy that way.

Many of the things you need to do to protect privacy are things you're already doing to meet other requirements, and many of the legal requirements are just good information management and common sense. You already have policies for the use and control of information; you already assess risks and respond to security incidents; you already train your staff for compliance with safety, security, and personnel regulations; you already handle customer inquiries and complaints; you already have policies describing standard clauses you put into your contracts with partners.

You can put together a fairly comprehensive privacy compliance program by making modest changes to these ongoing activities. You may need to appoint a privacy officer; you may need to develop new privacy policies, and you may need to write and publish a privacy notice. But you don't need to turn your business upside down, and you don't need to break the bank – if you work privacy compliance into your existing business processes.

Chapter 7

Other Issues



Does protecting data privacy undermine national security?

The rise of terrorism in recent years has led some people to question whether protecting individual privacy will weaken societal protections against violent attack. It's reasonable to be concerned about national security and personal safety, but an effective privacy protection program need not interfere with legitimate investigation of criminal activity.

The intent of privacy legislation worldwide is to protect the dignity of the individual person by requiring respectful and discreet handling of information about that individual.

Legal systems do not, as a rule, recognize a right to hide evidence of criminal activity from law enforcement authorities, and nor do they require any business to withhold information that is material to a criminal investigation from law enforcement authorities merely because that information would otherwise be considered private or personally identifiable.

Privacy regulations worldwide define standards for due process that must be met before law enforcement is granted access to personally identifiable information.

Generally, therefore, a privacy program that complies with applicable legislation should not interfere with law enforcement's ability to investigate criminal activity.

Privacy protection may in some cases improve national security and personal safety. For example, protecting the personal information used to identify individuals (national identification numbers, social security numbers, credit card numbers, etc.) may make identity theft and forgery of identification documents more difficult. This may make it more difficult for criminals to engage in clandestine activities.

Anonymity and pseudonymity

Personally identifiable information is information about *you*, in some fundamental sense. Guarding your privacy is, in a similar sense, protecting your identity. Your identity is obviously important, but there are times when you may need to drop your identity, or assume a false identity. These occasions need not be for nefarious purposes. For example, in an auction it is common for bidders to be identified only by a number, so that the market is influenced only by the offered price, and not by knowledge of another bidder's personal situation. Or in the situation of a whistle-blower or criminal informant – or just an employee who wants to make a suggestion – the public good may be served by allowing anonymity so information can be provided without embarrassment or fear of retribution.

Another example is an Internet chat room. Participants often adopt fanciful monikers that are more about who they would like to be than about who they are. It is generally clear to all concerned that these are pseudonyms, and in fact the ability to be pseudonymous may be part of the attraction of such sites.

So, you can see that sometimes it is useful to allow the use of "false" or untraceable identities. (We use "false" here in the sense of synthetic or artificial, not purposefully deceitful.) Sometimes these identities are truly anonymous, and don't allow the individual using them ever to be identified. More often, a pseudonym allows the person's true identity to be discovered only later, or on certain conditions, or through an intermediary. For example, the identity of a bidder in the auction will be revealed only if he wins. A person who uses a screen name in a chat room doesn't reveal himself to others in the chat room, but the operator of the chat room service may be able to trace him if necessary.

We bring up these situations only to note that anonymity and pseudonymity are not the same thing as privacy. Privacy is about the right to be you on your terms. Your rights to be anonymous, or to be someone else, are not as well developed or articulated as your right to privacy. Society is still struggling, as it has for centuries, with the competing notions of liberty and responsibility.

Do you need a Chief Privacy Officer?

We said earlier that your company needs a person to be accountable for the proper handling of personal information. Some larger companies have created a Chief Privacy Officer executive position, presumably to demonstrate the gravity of their concern for privacy. Should your company do that too? You probably don't need to.

We've emphasized throughout this Guide that respect for privacy is a part of everyday business. It's much more important to ensure that respect is built into your business than to invest someone with a fancy title. Make sure that there is always someone accountable for privacy as part of good business practice. And if questions are ever raised about your company's conduct concerning privacy, you will be able to show that you have good procedures, that you follow them, and that you can demonstrate that you do. If you can do that, no-one will care whether you've designated an employee to have that impressive job title.

There are some important functions, however, that *could* be fulfilled by a Chief Privacy Officer. Examples include assuring compliance with internal or external standards, or advocating for privacy issues inside or outside the company. Whether you need an explicit title for these is a business decision.

PKIs and other security technology

In the 1970s some clever researchers solved a vexing problem that had seriously impeded the practical use of cryptography. Without going into technical details, their innovation is called *public-key cryptography*, and it addresses the problem of distributing secrets (encryption keys) to large numbers of people without disclosing them in the process. Some later refinements added mechanisms for managing keys in the context of some business purpose. These mechanisms have come to be known as Public-Key Infrastructure (PKI).

It is fair to say that, at the outset of the twenty-first century, the promise of PKI has not yet been delivered. There are some security experts that believe it never will. Security products based on PKI do exist, however, and it's worthwhile to ask what impact they have on the notion of privacy.

The bottom line is mixed. PKI solutions can provide strong mechanisms for secrecy. For example, PKI can make it relatively easy for you to encrypt email to a correspondent and have reasonable confidence that it will not be intercepted and read by eavesdroppers. This is without doubt an improvement in privacy.

On the other hand, your use of PKI for security can – under certain circumstances – provide a company with a way to link you to an Internet interaction, even though you didn't enter any information about yourself. This sort of linkage is rarely useful to the company in the normal course of business, since it doesn't tell much about you. But it can be used as evidence to prove that you engaged in a transaction with the company. How compelling this evidence is depends on the technical sophistication of the audience. A jury might find it convincing, or they might discard it as mathematical gibberish. But the point is that the fact that the evidence exists is not necessarily good news for your privacy. It's almost certainly personally identifiable information, and therefore something that might be carelessly or maliciously disclosed.

Be wary of vendors that sell PKI as a privacy solution. That sword cuts both ways.

Biometric identification

Fingerprinting has been used to identify people for a long time. There are other biological signatures that may be used to uniquely identify an individual, with more or less precision. Ultimately, your DNA genome is in some sense a unique, permanent identifier. The question is, what does this mean for privacy? And the answer is, a lot.

Unlike a user ID and password, a biometric identifier can't be revoked, and you can't give it up and pick a new one whenever you want. For example, if your fingerprint is used to identify you, you can't later arrange for it to no longer be yours, unless you're willing to submit to some medical unpleasantness. (This is precisely why fingerprints are so useful for law enforcement purposes.) If the people you gave your fingerprint to then give it to others, those others may be able to identify you as well. You may then find that you have lost your ability to control your privacy. Circumstances such as these pose very real concerns about abuse of biometric identification data.

Surveillance and auditing

In your business, you have the need to protect your business, and ensure it is well run. To do this you may collect information outside your day-to-day business records. This information is easily overlooked when companies consider privacy. For example, you may have the need to perform surveillance of business operations (e.g., video monitoring of a warehouse to prevent theft). If this surveillance includes observations of employees or customers, it may be considered collecting personally identifiable information, and subject to legal regulation. It certainly may be a concern to those observed.

Another example is audit information. Audit records that are set aside for review outside the normal flow of customer interaction may still contain personally identifiable information. In some countries or jurisdictions, there are legal restrictions on the information that can appear in an audit file. At the very least, you should require some sort of extra step before transactions in an audit file can be associated with individuals.

Customer relationship management

In the face of all these privacy concerns, the term *customer relationship management* may sound like a disaster waiting to happen. After all, you can't manage a customer relationship without knowledge of the customer, and probably some knowledge that the customer might rather keep private.

You do need to be careful, but you don't need to stop doing what a smart businessperson does. Just take the words seriously: managing a relationship means understanding that needs, cares, and concerns go both ways in the best relationships. If you want to be on intimate terms with your customers, then act like an intimate.

Consent

The notion of consent is essential in privacy. You may sometimes hear the phrase "unambiguous informed consent". The two adjectives raise the bar – it's not enough to just have a signature. It's a good idea to get advice from experts in the law, as it applies to you, about what it takes for consent to be considered unambiguous and informed. You should get advice that takes into account what business you are in and where you are located. You may find that your trade or professional association, or a local chamber of commerce has already done the groundwork on this.

It's worth repeating here that you need consent, not only to collect information, but to use it for a particular purpose. Part of being informed means understanding the specific uses (and recipients) of information.

Be careful about negotiating too aggressively on privacy issues. Refusing to provide service unless a potential customer consents to questionable data collection practices may be seen in some jurisdictions as coercion. Coerced consent is not unambiguous consent.

Gossip and pillow-talk

With all the concern about computers and privacy, it's easy to forget that a great many compromises of privacy take place in direct human-to-human interactions. People discuss private information about others with their coworkers, friends, and family.

You probably can't make this stop altogether, but you can have clear policies (and associated reinforcements in training and communications) that remind your employees not to take privacy lightly. Like many other issues of corporate culture, respect for privacy comes straight from the top. If you're at the top, make it clear where you stand. If not, don't look for trouble.

Codes of practice and guidelines

Some industries have established codes of practice for privacy protection. You need to be aware of any such guidelines in your area, for two reasons. First, they may provide genuinely helpful guidance. Second, they provide a benchmark against which you will be compared if people start asking questions about your policies. If you don’t adopt your industry’s code of practice, you’ll need to be very clear about why not.

Your customer has a choice

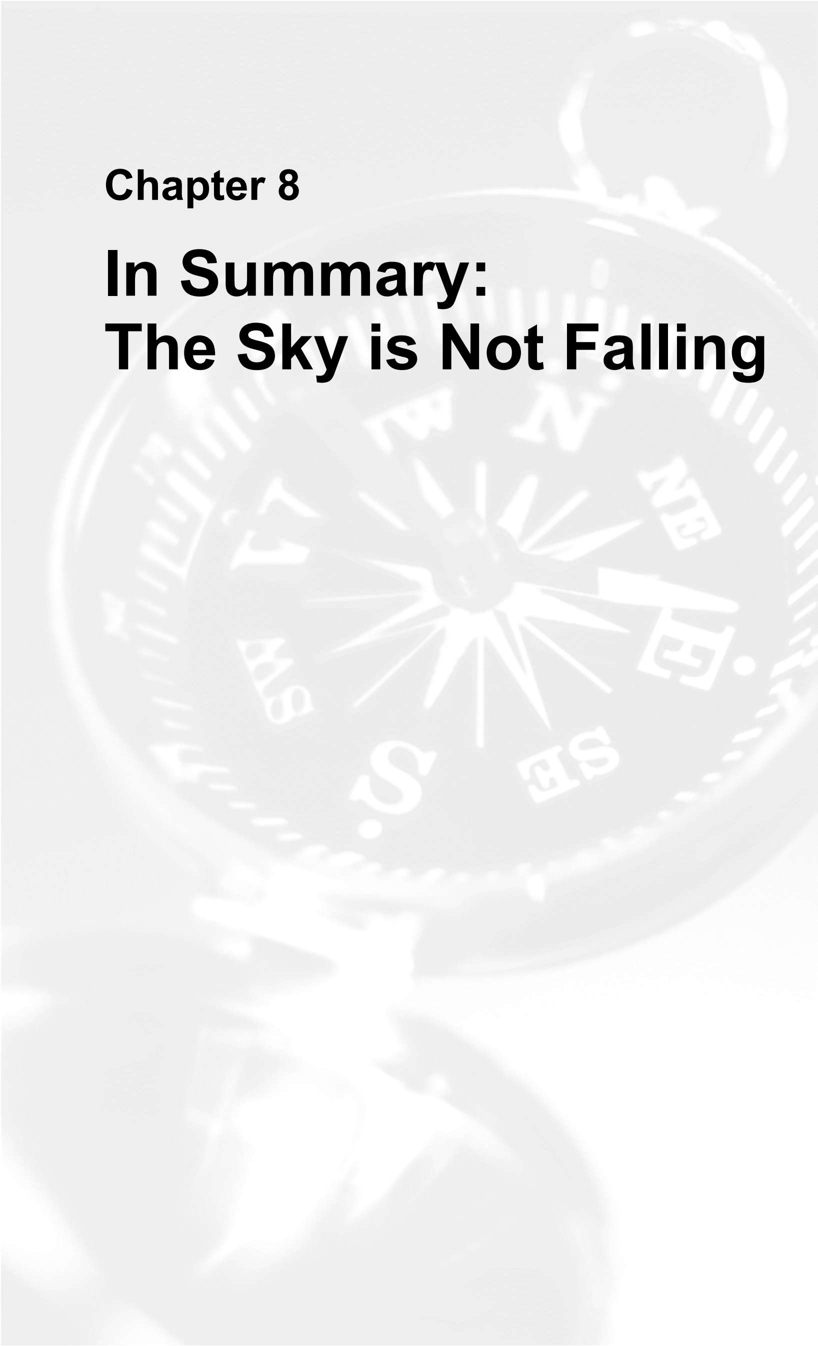
What does this mean to you as a businessman? How you address privacy can affect how people feel about doing business with you. If people are uncomfortable with the amount of privacy they feel they have to give up to you, they may simply choose to take their business elsewhere.

Do you appear to be intruding into a person's zone of privacy? Might it seem likely that information you have about your relationship with the customer will be shared? Could the identification techniques you use even vaguely remind a customer of Orwell's 1984? If your customer forms a perception that doing business with you will lead to a loss of his freedom to be and remain private he may choose to go elsewhere.

You have to demonstrate, in what you do, in how you explain what you do, and, especially, in what you choose not to do, that you will not intrude and that you will be respectful of privacy. And you have to show that you always allow your customer the freedom to reclaim any part of his privacy that he may give up to you in the course of your interactions.

Chapter 8

In Summary: The Sky is Not Falling



Do the right thing

We hope we've made it clear that privacy is a real issue, and that it's an issue not merely because there are legal requirements to safeguard it, but because your customers, employees, and partners care about their privacy. And while the issue of privacy is perhaps more prominent than it once was, that's not because people care more about privacy than they did before. It's because they believe there are greater threats to privacy now than ever before.

Fortunately, common sense is a pretty reliable guide to protecting privacy. If you as an individual are concerned about your personal information, then it's safe to assume that other people are concerned about theirs. And even if you'd be comfortable disclosing certain personal information, you can probably imagine how other people might not.

Sometimes you'll need to think hard, maybe with the help of consultants, about how personal information in your business might inadvertently leak out, or be stolen, or falsified. There are a lot of details to attend to, but the most important point is to establish the fundamental respect for privacy in both the policies and the actual conduct of business in your company.

Legal protections of privacy, with threats of fines or imprisonment, can't be taken lightly. You'll need to get advice from lawyers about what is required in your jurisdiction, and what is considered sound practice. (You may be able to get this advice from your trade or professional association.) We believe you'll find, however, that organizations that get into legal trouble over privacy transgressed the bounds of sound, ethical business practices long before they ever tangled with the law. Just doing the right thing goes a long way toward keeping you out of legal trouble, as well as in the black.

If you keep information about people in your business, you are probably going to be required to give them access to it. You can probably imagine that this might turn out to be a burden. If you're managing personal information well, you'll know exactly what you keep, and where to find it. You'll know who's in charge of maintaining it and whom to call if it's wrong. In other words, doing a good job of protecting privacy makes complying with this requirement easier. Even more importantly, being direct and forthright with the subjects of this information, keeping only the information you need, and using it only for agreed purposes, will help to keep the request load low. Remember that there is a cost to the user, at the very least in terms of their time, to request information and verify its accuracy. If you give them reason to feel confident in the quality of your information and the purposes to which it's used, they may find that their time is spent better on other, more pressing, concerns.

You can protect privacy the same way you do lots of things that matter in business: write down what you intend to do, make sure everyone understands that you mean it, *act* like you really mean it, check to make sure the right things actually get done, and move purposefully to fix any problems you find.

If you need to catch up

A good place to start if you are behind in attending to good data privacy practice is to find all the places where personal information is kept. If you don't need the information any more, get rid of it. The mere existence of this information presents business risk. If you're not getting business value for it, then you should eliminate the risk.

If you need to keep personal identification, begin taking steps to de-identify it. If you need to store customer names and addresses, don't store transaction histories in the same database. Use an opaque key to link the two databases together only when they need to be linked. Steps like this lower the risk that aggregated information will be misused.

If you have personal information and you need to keep it, but you did not have unambiguous informed consent to collect and use it, you should try to get consent after the fact.

If your business is too far behind the curve, consider engaging privacy consultants who understand your industry sector. Among other things, experts can help you to understand the best practices in your sector.

Chapter 9

Where Can I Learn More?

Web search engines will find huge numbers of links to "data privacy", even if you narrow the search to using additional search criteria. As usual, refining the search carefully helps greatly to find what you want.

The following list provides an initial starter set of recommended reading if you want to find out more about specific aspects of data privacy, both in its origins and in its evolution, and as it is applied in a variety of jurisdictions around the world.

❑ The OECD Privacy Guidelines:
www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

❑ The European Union Data Protection Act:
europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

❑ The U.S. Department of Commerce Safe Harbor Principles:
www.exports.gov/safeharbor

❑ The Canadian Personal Information Protection and Electronic Documents Act:
www.privcom.gc.ca/legislation/02_06_01_e.asp

❑ The U.S. Department of Health and Human Services HIPAA Privacy Rule:
aspe.hhs.gov/admnsimp

❑ The U.S. Senate Banking Committee Gramm-Leach-Bliley Act of 1999:
www.senate.gov/~banking/conf

❑ The U.S. Sarbanes-Oxley Act of 2002:
www.fmsinc.org/cms/?pid=3253

❑ EPIC (The Electronic Privacy Information Center):
www.epic.org

❑ Privacy.org:
www.privacy.org

index

About the Author(s)

Bob Blakley is chief scientist for Security and Privacy at IBM Tivoli Software. He is general chair of the 2003 IEEE Security and Privacy Conference and serves on the National Academy of Science's study group on Authentication Technologies and their Privacy Implications. He also serves on the editorial board for the International Journal of Information Security (IJIS).

Jacques Francoeur is founder and CEO of trustEra, Inc., who specialize in Enterprise Digital Trust Management (EDTM). Under his leadership, trustEra pioneered the field of EDTM and developed the Digital Chain of Trust Methodology (DCTM). He is also an Instructor of International Trusted eBusiness and Trusted eSystems at the University of California at Berkeley Extension.

Steven Jenkins is Principal Engineer to the Chief Information Officer at the Jet Propulsion Laboratory, California Institute of Technology. He advises JPL senior management on issues relating to information system engineering, and produces research and program plans to help JPL use information technology to accomplish its mission. He was also chair of The Open Group Security Forum between January 2000 and February 2003.

Eliot M. Solomon is Principal at Eliot M. Solomon Consulting, Inc., where he offers his expertise in development and analysis of IT strategy, following 15 years at the Securities Industry Automation Corporation (SIAC), where he became their first Distinguished Technologist and Vice President. He is also the founder and chair of the Securities Industry Middleware Council, Inc. (SIMC).

For information about **The Open Group Security Forum,** go to www.opengroup.org/security.