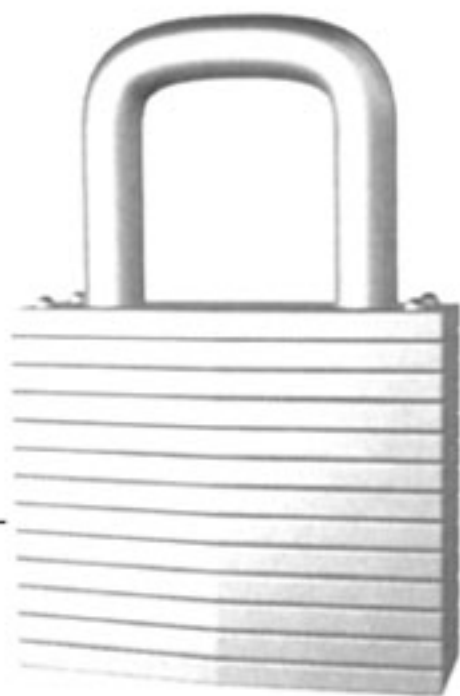


# NET PRIVACY

---

A  
guide to  
developing &  
implementing  
an ironclad  
**ebusiness**  
privacy plan



---

MICHAEL ERBSCHL OF  
JOHN VACCA

NET  
PRIVACY

*Net Privacy* is available in print and electronic formats.

[Click here](#) to:

- get more information about this book
- see formats available
- find out about related books
- e-mail a friend about this book

---

# NET PRIVACY

---

A GUIDE TO  
DEVELOPING AND  
IMPLEMENTING AN  
INTERNET EBUSINESS  
PRIVACY PLAN

MICHAEL ERBSCHLOE  
JOHN VACCA

**McGraw-Hill**

New York Chicago San Francisco Lisbon London  
Madrid Mexico City Milan New Delhi San Juan Seoul  
Singapore Sydney Toronto

# McGraw-Hill

A Division of The McGraw-Hill Companies



Copyright © 2001 by Michael Erbschloe and John Vacca. All rights reserved. Manufactured in the United States of America. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

0-07-138111-2

The material in this eBook also appears in the print version of this title: 0-07-137005-6.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill eBooks are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please contact George Hoare, Special Sales, at [george\\_hoare@mcgraw-hill.com](mailto:george_hoare@mcgraw-hill.com) or (212) 904-4069.

## TERMS OF USE

This is a copyrighted work and The McGraw-Hill Companies, Inc. (“McGraw-Hill”) and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill’s prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED “AS IS”. MCGRAW-HILL AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

DOI: [10.1036/0071381112](https://doi.org/10.1036/0071381112)

To Ronald Spangler for his inspiration, support, and friendship  
over the last 40 years and for changing my life forever  
by introducing me to the world of sci-fi.

—*John R. Vacca*

To my mother for her growing  
tolerance of her children.

—*Michael Erbschloe*

# CoNTENTS

*Foreword ix*

*Preface xiii*

*Introduction xv*

*Acknowledgments xix*

1	The Threat to Privacy and Corporate Vulnerability	1
2	The Nature of Privacy Problems	15
3	The Regulatory and Legislative Environment	30
4	Organizing to Protect Privacy	43
5	Conducting a Privacy-Needs Audit	55
6	Evaluating Technology Needs for Privacy Protection	67
7	Developing the Enterprise Privacy Plan	82
8	Implementing the Enterprise Privacy Plan	97
9	Managing Privacy on the Enterprise Web Site	115
10	Managing Privacy on Internet Supply Chains	130

11	Managing Privacy Efforts over the Long-Term	141
12	Protecting the Privacy of Enterprise Storage and Processing	152
13	Protecting the Privacy of Corporate Communications	173
14	Protecting Corporate Desktop Privacy	211
15	Protecting the Privacy of the Road Warrior's Laptop	246
16	Protecting the Privacy of Remote Access and Telecommuters	265
17	The Future of Privacy Management	293

*Glossary* 299

*Index* 311

## F◦R◦E◦W◦O◦R◦D

“The rules for conducting business today have changed.” That sentence isn’t news anymore, but it seems to be the magic phrase in every advertisement that touts the “ebusiness” revolution. Your own company has probably had a Web site for quite awhile, and everyone in your office probably conducts some sort of business through email or the Web. So what’s new about this statement?

Before the corporate marketers tacked on “e” to everything under the sun, marketing efforts were akin to breaking out the rifle and pith helmet to go on the hunt for customers. It required a tremendous effort to cultivate a prospect list, dispatch literature, track responses, and measure a campaign’s effectiveness. But now thanks to the almighty search engine, the tide has turned and customers are now hunting for you.

When customers find you, they will likely know more about your company than many of the people *in* your company do, and they’ve already scouted out your competitors. If they decide to do business with you, they will likely provide you with something even more valuable than their initial order: name, address, phone, email address, credit card number, and so on. Maybe they’ve provided the other jewels of the personal information crown like their favorite color, which type of carbonated beverage they prefer, or their pet snake’s birth date. So how have the rules for business changed? Your customers now know the value of this crown, and they won’t give it to just anyone.

As a Web manager, part of my job is to ensure that visitors to my site are comfortable with the security measures in place. I also

need to fortify the reputation of my organization by offering assurances that these visitors' personal information will not be misused. Even more importantly, the organization needs to religiously adhere to its own policies and educate its employees in the proper methods of securely handling personal information.

Most Web surfers are familiar with the lock that appears at the bottom of their browsers when performing a transaction. The lock shows that data sent to a Web site are being hidden from eavesdroppers. But what happens to those data once they have reached their destination? Misuse of a customer's personal information can be just as damaging to an organization's livelihood as an outside security breach. Security holes can be repaired quickly, but trust takes time to earn.

Regular reports of malicious hackers breaking into commerce Web sites have raised sensitivity to the risks involved in the adoption of ecommerce. Today's netizens are not only more aware of security issues, but they will want to establish a level of trust with whomever their information is shared. As the ease of identity theft and other information crimes increases, protecting our sensitive personal information becomes more vital. We need to know who has access to our information and how these data are being used.

Information security companies such as RSA have developed extremely effective ways of scrambling transmissions, encrypting and securely storing sensitive data, and adding safeguards to ensure that only those who are supposed to have access can view these data. But even the most bulletproof security measures can be rendered useless without solid policies behind them and proper implementations of those policies in place.

Whether you're on the server side or the browser side of the Web, you're off to a great start in expanding your knowledge of personal trust relationships with the online world . . . you're reading this book. *Net Privacy: A Guide to Developing and Implementing an Ironclad Ebusiness Privacy Plan* will greatly assist your organization in developing a privacy and security strategy. It provides a view of privacy issues from all sides and includes real-world situations involving privacy mistakes. It outlines legal issues and government regulations that effect policy decisions and provides checklists for implementing security procedures for most any organizational data-sharing situation.

If you're someone just concerned about online privacy, this book will provide a better understanding of how private information is

handled and how those data can be abused. It will give insight on what questions to ask when starting a trust relationship with any organization.

*Jason Thompson*  
Webmaster  
RSA Security, Inc.

[webmaster@rsasecurity.com](mailto:webmaster@rsasecurity.com)  
<http://www.rsasecurity.com/>

# PREFACE

Governments and businesses face three major challenges in dealing with the privacy of personal and corporate information—philosophical, legal, and procedural. The philosophical debate about what type of information is and should be private has raged on since the beginning of the industrial revolution and shows no signs of ending anytime soon. Since the growth of Internet communications and e-commerce, the legal definition and laws for the protection of privacy have become a tangled mess of international politics, corporate interests, rhetorical advocacy, and economic posturing. These processes will also continue and are likely to become increasingly messy over the next two decades. This book was written to address the procedural side of privacy protection and to provide organizations with a framework and process to develop, maintain, and implement appropriate policies and procedures to protect privacy.

Philosophical debates, especially when they are focused on something as sensitive as the privacy of individuals and the liberty that inherently emerges from the protection of that privacy, are stimulating and thought provoking. The process of enacting laws to protect privacy and the need for international cooperation in the millennium of the global Internet communications, economics, and e-commerce are challenges that are straining provincial mentalities and protectionist tendencies. This is the social and political environment in which organizations must struggle to develop policies and procedures to protect privacy while simultaneously attempting to maximize the use of enterprise information assets. The problems caused by the turmoil in the political and legislative environments

are compounded by rapidly evolving Internet technologies. Add to this mix a lack of human experience in coping with rapid change and dealing with the cross-culturalization of philosophies and laws and you have a perfect recipe for chaos.

This book provides managers with step-by-step guidance for developing enterprise privacy policies and procedures. These structured processes and steps can keep a privacy task force from getting lost in rhetoric and overwhelmed by the chaos being created by macro political and economics forces. The basic foundation of the privacy management process is *governance*. As privacy policies are being formulated, governance allows the voicing of all of the perspectives necessary for organizations to successfully accomplish their missions and goals to be heard. A governance approach is necessary because enterprise privacy policies must be balanced to simultaneously meet legal requirements while maximizing the value of information assets. A motivated privacy task force and rational leadership are key to successful privacy management. Also the entire enterprise must be involved in the development and implementation of privacy policies and procedures. In addition to providing a governance framework, this book explains the practical procedural steps of establishing a privacy task force, evaluating privacy needs, formulating privacy policies, devising specific procedures to protect privacy, implementing and testing procedures, and monitoring and modifying privacy protection in the future.

All organizations will face privacy management issues, and, as laws evolve, all organizations could face civil or even criminal litigation for failing to properly protect privacy. Those organizations that have worked to develop privacy policies and procedures must remain vigilant to avoid negative consequences as laws, business relationships, and social conditions change. Those organizations that have not yet established privacy policies and procedures need to start doing so immediately.

*Michael Erbschloe and John Vacca*

# INTRODUCTION

The philosophical focus of this book's privacy management perspective is geared toward the improvement of the business bottom line for private companies and improvement of costs control and resource optimization for nonprofit and government organizations. The book contends that all types of organizations need to develop privacy policies that maximize the benefit of reusing information in as many ways as possible, while minimizing the risks associated with potential privacy violations. Although this balance is essential in an information-intensive world, clearly, organizations will not easily achieve the balance between privacy and the optimization of resources.

The Internet has contributed to the awareness of privacy issues in four ways. First, the Internet has resulted in a huge increase in the number of people using computers to seek information and make purchases. Second, several privacy-related incidents have resulted in considerable and less than favorable press coverage for enterprises that have suffered from privacy problems. Notably, in late 1999 and early 2000, Web technology that tracks how people use the Internet came under fire. Third, many organizations had their first experiences in dealing with large-scale privacy issues. They range from small, new Web-based companies to large enterprises that started using the Internet for marketing, sales, or information dissemination. Fourth, the global cross-border nature of the Internet presented totally new challenges to governments and enterprises. The combination of these trends set the stage for potential privacy conflicts.