ELSEVIER
SCIENCE

MAILING INSTRUCTIONS FOR AUTHOR'S MASTER PROOFS

Within 48 hours, please proofread and return master proofs to:

Sarah Manchester
Project Manager
Elsevier
200 Wheeler Road, 6th Floor
Burlington, MA 01803
Ph: 781-313-4806
F: 781-313-4880
s.manchester@elsevier.com

For authors inside the United States: Please ship via express courier (Federal Express, Airborne, UPS, etc.) or first-class mail.

For authors outside the United States: Please ship via express courier only (i.e., the fastest service available). Slower means of delivery could lead to delays in publication.

forms/mailin.doc

Instructions to Authors for Correcting PDF Page Proofs

Note: These instructions are important. Please take the time to read them carefully.

The instructions listed below will aid in the accurate correction of this title's page proofs at minimum cost. A list of common proofreaders' marks is attached at the end of these instructions.

WHAT TO RETURN

The compositor has provided page proofs of your article in PDF format. Please print out the file and make corrections on the hard copy. After you make corrections, please return the original printout of your corrections to Academic Press; faxing them is acceptable if your corrections are few and easy to see after being faxed. All corrections should be made on these master page proofs. You may want to make a photocopy of your corrected proofs for your files.

HOW TO CORRECT PAGE PROOFS

1. Proofread the page proof. You are solely responsible for reading and correcting the material. Academic Press does not proofread material after it has been returned. Corrections may be written on a separate sheet or in a letter indicating the page number and precise location where each correction is to be made.

2. Mark corrections clearly in two places:

   In the text line. Where the correction is to be made, insert a caret (^), or one of the appropriate marks listed on the attached page, or just cross out the incorrect material.

   In the margin of the proof. Call attention to the correction and indicate what is to be done. In the margin, write the material to be inserted or explain what needs to be done, using proofreaders' marks if possible. However, any clear method of marking proofs may be used, provided it is logical and consistent. Do not cut proofs apart for any reason. Please initial the upper corner of each proof page after you finish it.

Note: When marking proofs, write legibly! Please use a distinctively colored pen or pencil when marking proofs.

3. Mark printer's errors. If a mistake in the proof was not in the manuscript, it is a "printer error" and will be corrected at the typesetter's expense. Please mark these corrections as "PE."

4. Answer all queries. Our copy editor's queries have been transferred to the typeset proofs. If no change is needed, write "OK as set" on the proof and cross out the query. If you do not agree with the editor's change, please mark your corrections in the margin and cross out the query.

5. Check running heads and page numbers for accuracy.

6. Check any cross-references to other chapters for accuracy.

7. Compare figures with legends to ensure agreement. If you have questions or concerns regarding your artwork, please note them on the master proofs.

8. Update any references that are not yet complete.

COST OF ALTERATIONS AFTER MANUSCRIPT IS TYPESET

It is customary for the publisher to assume the cost of corrections up to 15% of the total cost of composition. **Alterations in excess of this amount *will be charged to your account* unless the excess is the result of Academic Press or printer errors, or changes not attributable to you.**

Changes in typeset material cost $1.50 or more per reset line. A single change that necessitates resetting a complete paragraph may cost $15 or more. *If the total number of corrections averages more than 1 to 2 lines being reset for each page, the charge will probably exceed 15% of the cost of composition.*

How to Keep Costs to a Minimum

1. Avoid unessential changes such as insertion or deletion of words or punctuation that does not alter the meaning.

2. If you substitute a word or phrase, insert a substitution of a length similar to that of the deleted material whenever possible.

3. Transposing words, sentences, or phrases is costly, as is moving material from one page to another, which often results in changes to the indexes and front matter.

4. Avoid changes in structural formulas, tables, displayed math, and other illustrative material—these are costly changes.

Authors, editors, and printers use proofreader's marks to indicate changes on printed proofs. These standard marks are used in pairs, one in the text where the change is to be made and one in the margin closest to the change.

Mark in the margin	Mark in typeset text
	delete; take it out
	close up; print as one word
	delete and close up
a word	caret; insert here
	insert a space
	space evenly where indicated
	let marked text stand as set
	transpose; change order the
	used to separate two or more marginal marks and often as a concluding stroke after the final of several marginal marks
	set farther to the left
	set farther to the right
	align on margin
	imperfect or broken character
	indent
	begin a new paragraph
	spell out (set 2 as two)
	the printer will underline or circle a typeset word (or words) to alert the author that the copy may be incorrect but has been set as typed on the manuscript
	set in capitals (CAPITALS)
	set in lowercase (lowercase)
	set in italic (*italic*)
	set in roman (roman)
	set in boldface (**boldface**)
	insert hyphen (self imposed)
	superscript (2 as in χ^2)
	subscript (2 as in H_2O)
	centered (· for a centered dot in $p \cdot q$)
	insert comma (yes whereas)
	insert apostrophe (editors')
	insert period (end Then)
	insert semicolon (this in)
	insert colon (Tests Part 1)
	insert quotation marks (less than comparative)
	insert parentheses only two
	insert brackets (these 12 subjects)

ACADEMIC PRESS

525 B STREET, SUITE 1900, SAN DIEGO, CALIFORNIA 92101-4495
TELEPHONE (619) 699-6473 FAX (619) 699-6305 EMAIL l.pawlak@elsevier.com

ORDERING INSTRUCTIONS: please fax completed order form *and* mail original (with purchase order, if necessary) to the attention of: Lisa Pawlak

Order for Book Chapter Reprints

TITLE OF BOOK: New Economy Handbook	
EDITOR(S): **Derek Jones**	
AUTHOR(S):	
TITLE OF CHAPTER:	No. of pages in Chapter:

0 COPIES GRATIS

- **PRICES INCLUDE POSTAGE**
- **TAX EXTRA**

NUMBER OF REPRINTS TO BE PURCHASED:

_____ **Copies** $ _____
Cost for Color $ _____

Total Due $ _____

THE ABOVE ORDERED REPRINTS ARE TO BE **INVOICED** TO:

NAME _____
DEPARTMENT _____
DIVISION _____
INSTITUTION _____
STREET _____
CITY _____ STATE _____ ZONE _____
COUNTRY _____

INSTITUTIONAL PURCHASE ORDER
No. _____
☐ **is attached** ☐ **not necessary**
☐ **will be transmitted separately**

CREDIT CARD PURCHASE
☐ MC ☐ VISA ☐ AMEX
No. _____
EXP. DATE _____
SIGNED _____

E-MAIL _____ TEL. NO. _____ FAX NO. _____

Purchase orders for payment of reprints by an institution must be indicated on this order form.

SHIPPING LABEL **(Please TYPE or PRINT clearly)**

Name		
Dept.		Rm. No.
Division		
Institution		
Street	PO BOX NOT ACCEPTABLE	
City	State	Zone
Country		

Include any *special instructions* here:

ORDER YOUR REPRINTS NOW!

Take advantage of the opportunity to order chapter reprints at the best prices.

Why Order?

Make the most of your hard work!

- Lectures/appearances
- Commercial solicitation
- Pharmaceutical interest
- Promotional material
- Course adoptions
- Corporate sales
- Generate further interest in your book

Do not delay in ordering your reprints! Timing is crucial! To take advantage of the prices given below, please send in your orders **within one week**.

IMPORTANT

Minimum order: 50 copies (not including gratis copies).

Order form enclosed. Prices quoted do not apply to orders received after the book has been printed.

Please **use our order form** and **fill it out completely**.
Return our order form even if no reprints are desired.

Please fax and mail order form to:
Book Chapter Reprints, Academic Press, 525 B St., Suite 1900, San Diego, CA 92101-4495
Fax: (619) 699-6305

Academic Press Book Chapter Reprint Price List

COPIES: / *PAGES*	*50*	*100*	*200*	*300*	*400*	*500*	*600*	*700*	*800*	*900*	*1000*
1-2	$ 90	$ 155	$ 280	$ 395	$ 500	$ 600	$ 685	$ 760	$ 825	$ 880	$ 925
3-4	105	190	345	490	620	735	835	925	1,000	1,060	1,105
5-6	125	220	410	575	730	865	980	1,080	1,165	1,230	1,280
7-8	140	255	470	665	840	1,000	1,130	1,245	1,335	1,405	1,455
9-10	160	285	535	760	955	1,130	1,280	1,405	1,505	1,580	1,635
11-12	175	320	600	850	1,070	1,265	1,430	1,570	1,680	1,760	1,810
13-14	195	355	665	940	1,185	1,400	1,580	1,730	1,850	1,935	1,990
15-16	210	390	730	1,030	1,300	1,530	1,730	1,890	2,015	2,110	2,165
17-18	230	425	790	1,120	1,410	1,665	1,875	2,050	2,185	2,285	2,345
19-20	250	455	855	1,210	1,525	1,795	2,025	2,210	2,355	2,460	2,520
21-22	260	465	880	1,250	1,575	1,855	2,095	2,290	2,440	2,545	2,605
23-24	265	475	905	1,290	1,625	1,920	2,165	2,365	2,520	2,630	2,690
25-26	275	485	930	1,325	1,675	1,980	2,235	2,440	2,600	2,715	2,780
27-28	285	490	955	1,365	1,730	2,040	2,305	2,520	2,685	2,800	2,865
29-30	295	500	980	1,405	1,780	2,100	2,375	2,595	2,765	2,880	2,950
31-32	305	510	1,005	1,445	1,830	2,165	2,445	2,670	2,845	2,965	3,035
add'l 1-2	$ 10	15	30	45	55	65	75	80	85	90	90

PRICES INCLUDE SHIPPING AND HANDLING

IF COLOR ILLUSTRATIONS ARE REPRODUCED IN YOUR CHAPTER, ADD $100.00 PER 100 PURCHASED REPRINTS ($50.00 FOR FIRST 50 COPIES).

Contents

19	E-Money and Payment Systems	Good		
20	Accounting Issues in the New Economy	Wallison		
21	New Electronic Trading Systems in Foreign Exchange Markets	Rime		

Section IV : Labor Markets

22	The Internet and Matching in Labor Markets	Kuhn		
23	Who Uses Computers and In What Ways: Effects on Earnings Distribution	Gittleman	Handel	
24	The New Economy and the Organization of Work	Black	Lynch	
25	Skill Based Technology Change in the New Economy	Machin		
26	The New Economy and the Impact of Immigration and the Brain Drain	Schmidt	Rothgang	
27	The New Economy and Forms of Compensation	Klinedinst		

Section V : Entrepreneurship

28	Regional Origins of the New Economy	Norton		
29	Venture Capital in the New Economy	Guilhon	Montchaud	
30	Business Models in the New Economy	Ehrmann		

Section VI : Macroeconomics and Growth

31	Growth and Innovation in the New Economy	Stiroh		
32	International Productivity Convergence in the New Economy: More or Less Likely?	Lutzker		
33	The New Economy and Business Cycles	Louçã		

Section VII : Policy and Institutional Framework

34	Macro Policy-Making in the New Economy	Baker		
35	The Digital Divide and What to Do About It	Hargittai		
36	Property Rights in the New Economy	Park		
37	Taxation and the New Economy	Wiseman		
38	Regulation and the New Economy	Lee		
39	Privacy (E-Snooping) and Security in the New Economy	Ackerman	Treese	David
40	Policy Issues and the New Economy for Developing and Transition Economies	Mann		

41	The New Economy and International Trade	Kleinert	Schuknecht
42	Intellectual Property Rights in the New Economy	Andersen	
43	International Governance of the Internet: An Economic Analysis	Brady	
44	E-Learning	Weller	
45	Trust in the New Economy	Putterman	Ben-Ner

Chapter 39

Privacy and Security Issues in E-Commerce

Mark S. Ackerman*
*School of Information and
Department of Electrical Engineering
and Computer Science,
University of Michigan

Donald T. Davis, Jr.†
†Cryptographer and Security Consultant,
Somerville, MA

Privacy—the control over one's personal data—and security—the attempted access to data by unauthorized others—are two critical concerns in the "new economy". Consumers are concerned about their personal data leaking unexpectedly or uncontrollably, and e-commerce sites fear the financial losses associated with bad publicity, unauthorized access, and break-ins. This chapter discusses the business, social, and economic issues surrounding both privacy and security. This chapter also surveys the technologies that can be incorporated or have been proposed for both. © 2003, Elsevier Science (USA).

New Economy Handbook

Computer security The effort to control the use, confidentiality, and authenticity of electronic data and to guarantee the availability and authorized use of computers, networks, peripherals, and other electronic resources.

Digital signature A cryptographic tag that only one author can calculate; the tag can be combined with any kind of data that the author might create (e.g., financial, entertainment, medical), and the tag's validity can be checked by anyone who can access the data.

Platform for privacy preferences (P3P) A labeling protocol that describes a Web site's uses for personal data (including clickstream data). Users can also describe their data dissemination preferences.

Privacy The ability of an individual to control the terms under which her personal information is acquired and used.

Privacy-enhancing technologies (PETs) Technology-based solutions that attempt to defeat or neutralize surveillance or tracking technologies.

Public key infrastructure (PKI) A flexible encryption key distribution system in which every participant carries two cryptographic keys, one for encryption (called the private key) and one for decryption (called the public key).

Symmetric key system A key system in which the same key is used for both encryption and decryption, so the key must always be guarded as a secret.

I. INTRODUCTION

Privacy—the control over one's personal data—and security—the attempted access to data by unauthorized others—are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both. This chapter reviews the current state of the art and the relevance for privacy and security, respectively. We examine privacy from social–psychological, organizational, technical, regulatory, and economic perspectives. We then examine security from technical, social and organizational, and economic perspectives.

II. PRIVACY

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher (2001) reported that "Forty-one percent of Web buyers surveyed last year by Forrester Research of Cambridge, Mass., said

they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely." A *Business Week*–Harris Poll found that over 40% of on-line shoppers were very concerned over the use of personal information, and 57% wanted some sort of laws regulating how personal information is collected and used (Harris Poll, 2000). Similarly, Culnan (2000) argued that privacy concerns were a critical reason why people do not go on-line and provide false information on-line.

Why this concern about privacy? The answer is simple. As of 1998, the Federal Trade Commission (FTC) found that the majority of on-line businesses "had failed to adopt even the most fundamental elements of fair information practices" (Culnan, 2000). Indeed, relatively few consumers believe that they have very much control over how personal information revealed on-line is used or sold by businesses (Culnan and Armstrong, 1999). The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce.

Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right, whereas others consider it to be a tradable commodity. Detailed arguments about the historical progression of privacy can be found, for example, in Davies (1997) and Etzioni (1999). (Even these historical accounts have sharply differing viewpoints. For example, Etzioni argues that privacy is societally illegitimate or not feasible, whereas Davies argues that it has become a squandered right.) For the purposes of this chapter, we will explore the potential space of privacy concerns, not privileging any particular viewpoint. In our view, both consumers and businesses may have legitimate viewpoints, sometimes conflicting. This is in the nature of most societal issues. We also restrict ourselves to the privacy issues that accrue in electronic commerce; we omit, for example, the issues emerging from vehicle tracking chips, the wholesale monitoring of telephone and other communication mechanisms, and image recognition from public cameras [see Froomkin (2000) for other examples].

Culnan (2000), following Westin, defines privacy as "the ability of an individual to control the terms under which their [*sic*] personal information is acquired and used." An individual's privacy, as such, is always in an inherent state of tension, because it must be defined in conjunction with the capabilities of others to transact business and even to control their own privacy. As Clarke (1999) noted, privacy may have to be traded off in certain transactions, such as to access credit or to maintain the quality of health care. Indeed, societal needs may also transcend an individual's privacy concerns, as in the case of public health.

Nonetheless, individuals as e-commerce consumers, even with its inherent trade-offs, still wish to control their personal information. Goffman (1961) noted that people must control their presentation of self, their face, to others. People need to be able to control what others think of them and find it disconcerting when they cannot. Even more, people find it disconcerting when the rules of everyday conduct appear to change, as they can with new technologies. In these situations, people may feel that they have been treated unfairly or that they have not received proper notice (Culnan, 2000).

Besides "privacy," a number of terms, such as notice, choice, identification, digital persona, authentication, anonymity, pseudonymity, and trust, are used in privacy discussions. However, because of space limitations, we cannot hope to carefully define each. See Clarke (1999) for a useful introduction. Note, however, that there is a vigorous research debate surrounding many of these concepts.

A. Social and Business Issues

Why is privacy of concern to e-commerce? We believe this concern stems from a new technical environment for consumers and businesses, the resulting data flow with substantial benefits to businesses and consumers, consumer concerns in this new environment, and regulatory attempts to govern this environment. It is important to understand each one of these and to understand the trade-offs. Privacy as a business issue is extremely sensitive to changes in the surrounding context. Changes in people's expectations (such as when they become accustomed to data transfer in commercial settings) or in regulatory governance (such as new laws, governmental regulations, or even case law in the United States) can dramatically alter business issues and possibilities.

Following is an overview of the research and business issues. This will include the consumers' concerns, technical issues, and regulatory attempts to ameliorate privacy concerns. In this examination, our attempt is not to predict what will happen or should happen, but to present issues to guide further research and business activity.

Clearly, there are many business opportunities in the changing technical environment. The use of digital systems allows data to be captured at a much greater rate and scope than previously; e-commerce sites potentially could collect an immense amount of data about personal preferences, shopping patterns, patterns of information search and use, and the like about consumers, especially if aggregated across sites. Not only is it easier than ever to collect the data, it is also much easier to search these data (Dhillon

and Moores, 2001). New computational techniques allow data mining for buying patterns and other personal trends. These data can be used to personalize a customer's e-commerce experience, augment an organization's customer support, or improve a customer's specific e-site experience. The data are valuable for reuse, for example, in finding potential sales to existing customers. In addition, the data are also valuable to aggregators (who may look for other personal trends and patterns) or for other types of resale. Indeed, reuse and resale are simultaneously both potential opportunities and potential problems. "Ironically, the same practices that provide value to organizations and their customers also raise privacy concerns" (Culnan and Armstrong, 1999).

From the viewpoint of customers, many e-commerce sites have done foolish things with their customers' data (Fisher, 2001). Consumers' opinions on this have been confirmed by media stories of particularly egregious privacy failures and public relations nightmares. Broadly speaking, consumers are merely confirmed in their opinions by the media. As mentioned, few consumers trust companies to keep their data private. In one survey, 92% of respondents indicated that, even when companies promised to keep personal data private, they would not actually do so (Light, 2001).

Culnan and Armstrong (1999) make the argument that consumers have two kinds of privacy concerns. First, they are concerned over unauthorized access to personal data because of security breaches (see following discussion) or the lack of internal controls. Second, consumers are concerned about the risk of secondary use: the reuse of their personal data for unrelated purposes without their consent. This includes sharing data with third parties who were not part of the transaction in which the consumer related his personal data. It also includes the aggregation of a consumers' transaction data and other personal data to create a profile. Smith *et al.* (1996) raise two additional concerns based on Delphi studies: general concerns about personal data being collected and concerns over one's inability to correct any errors.

Beyond the research literature describing a general anxiety (and its extent), there is some research literature providing more detail. A persistent finding, over several decades, is that it is fruitful to consider U.S. consumers not as a general block but as consisting of three groups (Westin, 1991): privacy fundamentalists, the pragmatic majority, and the marginally concerned. These groupings have been consistent across studies [e.g., Ackerman *et al.* (1999), Spiekermann *et al.* (2001)]. [Spiekermann *et al.* (2001) divided the pragmatics into those who were concerned with revealing their identity and those who were more concerned about making their personal profiles available.] In Ackerman *et al.* (1999), these groups were

17%, 56%, and 27% of the sample, respectively. Spiekermann *et al*. (2001) noted a larger group of privacy fundamentalists and fewer marginally concerned in Germany. The groups differ significantly in their privacy preferences and attitudes. The marginally concerned group is mostly indifferent to privacy concerns; privacy fundamentalists, on the other hand, are quite uncompromising about their privacy. The majority of the U.S. population, however, is concerned about its privacy, but is willing to trade personal data for some benefit (e.g., customer service). Nonetheless, consumers still want adequate measures to protect their information from inappropriate sale, accidental leakage or loss, and deliberate attack (Dhillon and Moores, 2001). In Ackerman *et al*. (1999), the concerns of pragmatists were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on Web sites.

Another interesting finding, also quite persistent, is that there is a large gap between most people's stated preferences and their actual behavior (Ackerman *et al*., 1999; Spiekermann *et al*., 2001). Although this is often the case in social studies (Bernard, 2000), it is of particular interest here. It is not yet known, however, whether this gap is permanent, in that it is unlikely to change, or is the symptom of people's frustration with current technologies.

B. Technologies for Privacy

The next consideration is technology. A number of technologies have altered the current privacy debates. Clarke (2001) divides the technologies in question into four groups. Clarke argues that there are technologies used for surveillance, technologies for forming agreements (contracting) about the release of private data, technologies for labeling and trust, and privacy-enhancing technologies (PETs).

The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of endangering personal privacy. These include generating data trails, data warehousing and data mining, and biometrics. Many of these technical mechanisms can lead to consumer profiles that "are no longer based only on the individual's dealings with a single organization, because their [*sic*] data is shared by multiple merchants" (Clarke, 2001).

Balancing these tracking mechanisms are privacy-enhancing technologies (PETs), which attempt to defeat or neutralize the surveillance or tracking technologies. Basic PETs include cookie managers and personal firewalls. Other PETs attempt to provide genuine anonymity and include anonymous remailers (e.g., Mixmaster) and digital cash (e.g., ECash). An

active area of research and development are systems to provide nontraceable identifiers (e.g., ZKS Freedom, AT&T Crowds, anonymizer.com, anonymous remailers). Yet other PETs, which Clarke (2001) calls "gentle PETs," try to balance privacy and accountability. These include systems to provide some level of pseudonymity, allowing users to hide behind pseudonyms but allowing actions to be traced back to a person if necessary. In addition, privacy seals (e.g., from TRUSTe or the Better Business Bureau) indicate that the company follows the privacy practices stated on its Web site.

A new area of research includes the so-called labeling protocols, such as the MIT–World Wide Web Consortium's Platform for Privacy Preferences (P3P) (Cranor and Reagle, 1998; Cranor, 2002; P3P, 2002). P3P allows sites to describe their data handling policies (P3P statements) and permits users to describe their preferences for releasing private data (P3P preferences). As sites label themselves with P3P and as user clients (such as Internet Explorer) handle P3P statements and preferences, it will be possible to create technologies to form contracts for the release of private data. Other technologies, such as those to help users understand contractual terms or even contract-related fraud, will also emerge. Ackerman and Cranor (1999) outline one such technology. Their browser-based agents watch for privacy violations, privacy scams, and the like on behalf of the user.

C. Regulation, Economic Issues, and Privacy Codesign

The final consideration is regulation. In this, we include the varying governmental attempts, whether by law or by decree, to regulate this new environment on behalf of their citizens. It also includes emerging legal precedents and case law for governing privacy in cyberspace. Currently, regulation is a warren of overlapping and conflicting attempts. Fortunately, these attempts are slowly consolidating. (Around 1997, it was thought possible that even municipalities might have their own, specific privacy regulations, holding ISPs and Web services responsible for any violations.) Nonetheless, currently there are wide differences between the United States and the European Union. To continue e-commerce, the notion of a "safe harbor" has emerged internationally, although it is not known how long this will continue.

In the United States, privacy is largely a matter of economics, with the admonition that caveat emptor is the rule for consumers. Once data are provided by an individual to an e-commerce site or anyone else, all rights

to that data are lost. U.S. consumers have no recourse, which may result in surveys showing a lack of trust. A company can use these data in any way, including selling the data to third parties for subsequent reuse. There are, however, specific areas of greater protection, for example, in medical records. In addition, the Federal Trade Commission (FTC), which regulates consumer and interstate trade in the United States, has taken upon itself to take particularly egregious privacy cases to court. For example, the FTC has taken large companies to court when they have violated their own sites' privacy statements. Although many researchers and analysts [e.g., Reidenberg (1999), Culnan (2000)] have argued that self-regulation has largely failed, it is unlikely that there will be significant change under the current U.S. administration. It is possible, however, that greater penalties may accrue to companies violating their own privacy statements.

In contrast, "Privacy rules are strikingly different in the European Union, and the differences threaten to hamper the ability of US companies to engage in transactions with European Union countries without risk of incurring penalties" (Fjetland, 2002). Europeans must unambiguously give consent after being informed as to why the information will be used; this is not the case in the United States. According to European Union rules, consumers must be informed of the entity collecting the data, purposes of the processing, recipients of the data, and any rights they (the customers) have. Furthermore, one must ask for specific consent for "sensitive information" (a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual preference). Unlike in the United States, European customers can have incorrect or unlawfully processed data corrected, blocked, or erased, and consumers can even require that third parties who have seen incorrect data be notified.

The extent to which European Union privacy rules hold for companies is unclear. Technically, not only do the European Union rules apply to European Union citizens, but they also apply even if the customer is outside the European Union if the data will be processed within the European Union. The onus is on the data user (i.e., the company or electronic commerce site), and the penalty can be the blockage of data transfers to the offending company. Currently, however, these European Union rules are suspended for American and international companies, and little if any enforcement is occurring for European Union companies. Not even all European Union countries have complied (Fjetland, 2002). As a "safe harbor," which has been the point of contention between the U.S. and European Union governments, U.S. and international companies must merely embrace a substantially diluted version of the privacy standards.

Thus far, we have largely examined privacy from a sociological stance, that is, as socially constructed expectations and sets of norms and regula-

tions. Privacy can also be thought of as an economic good. Considerable research has examined a marketplace for personal data. A general analysis of markets for data, including personal data, can be found in Shapiro and Varian (1999). An example of potential economic mechanisms for privacy data markets, including negotiation protocols, can be found in Cranor and Resnick (2000).

Very recently, researchers have moved toward advocating approaches to privacy that combine technology, regulation, and social change. The technologies may include economic mechanisms. Increasingly, privacy is considered a complex social phenomenon with interactions among new technologies, regulatory structures, and citizens' perceptions of privacy and social norms. Reidenberg (1999) and Cranor and Reagle (1998) have argued that e-commerce privacy requires a combination of law and technology, and Ackerman *et al*. (2002) have argued that solutions for privacy must simultaneously consider technology, social structures, and regulation in a codesign space.

III. SECURITY

As mentioned, security is also a major concern for e-commerce sites and consumers alike. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. We will cover each in turn.

A. Security Vulnerabilities in Electronic Commerce

There are many points of failure, or vulnerabilities, in an e-commerce environment. Even in a simplified e-commerce scenario—a single user contacts a single Web site and then gives his credit card and address information for shipping a purchase—many potential security vulnerabilities exist. Indeed, even in this simple scenario, a number of systems and networks are involved. Each has security issues.

First, a user must use a Web site and at some point identify, or authenticate, herself to the site. Typically, authentication begins on the user's home computer and its browser. Unfortunately, security problems in home computers offer hackers other ways to steal e-commerce data and identification data from users. Some current examples include a popular home-banking

system that stores a user's account number in a Web "cookie," which hostile Web sites can crack (Graves and Curtin, 2000), ineffective encryption or lack of encryption for home wireless networks (Borisov *et al*., 2001), and mail-borne viruses that can steal the user's financial data from the local disk (Roberts, 2002) or even from the user's keystrokes (Neyses, 2002). Whereas these specific security problems will be fixed by some software developers and Web site administrators, similar problems will continue to occur. Alternatives to the home computer include point-of-sale (POS) terminals in bricks-and-mortar stores, as well as a variety of mobile and handheld devices.

Second, the user's Web browser connects to the merchant on the front end. When a consumer makes an on-line purchase, the merchant's Web server usually caches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit card fraud. Further, such archives often hold 90 days' worth of customers' orders. Naturally, hackers break into insecure Web servers to harvest these archives of credit card numbers. Several recent thefts netted 100,000, 300,000, and 3.7 million pieces of credit card data. Accordingly, an e-commerce merchant's first security priority should be to keep the Web server's archives of recent orders behind the firewall, not on the front-end Web server (Winner, 2002). Furthermore, sensitive servers should be kept highly specialized by turning off and removing all nonessential services and applications (e.g., ftp, e-mail). Other practical suggestions to secure Web servers can be found in Tipton and Krause (2002), Garfinkel (2002), and Garfinkel *et al*. (2003), among many others.

Third, the merchant back end and database. A site's servers can weaken the company's internal network. This not easily remedied, because the Web servers need administrative connections to the internal network, but Web server software tends to have buggy security. Here, the cost of failure is very high, with potential theft of customers' identities or corporate data. Additionally, the back end may connect with third party fulfillment centers and other processing agents. Arguably, the risk of stolen product is the merchant's least important security concern, because most merchants' traditional operations already have careful controls to track payments and deliveries. However, these third parties can release valuable data through their own vulnerabilities.

This is a simplified model of e-commerce architecture, yet even in its simplicity there are a number of security problems. Note that encrypted e-commerce connections do little to help solve any but network security problems. Whereas other problems might be ameliorated by encryption, there are still vulnerabilities in the software clients and servers must use for the data. We will discuss the implications of these vulnerabilities next: users

who may themselves release data or act in ways that place sites at jeopardy, the constant pressure of new technologies, and the resulting constant threat of new vulnerabilities, as well as the requirements for critical organizational processes. However, before discussing potential requirements for e-commerce sites and their consumers, it is important to survey potential security technologies.

B. Security Technologies

There are many relevant technologies, including cryptographic technologies, that can mitigate the Preceding vulnerabilities. However, none is comprehensive or airtight by itself. Accordingly, we next present a brief overview of the major technologies and also consider the advantages and disadvantages of each. For a more complete description of each technology, see Bishop (2003).

In the mass media, the most visible security technologies are the encryption algorithms. For a general introduction to these technologies, see Treese and Stewart (1998); a popularization can be found in Levy (2001). Two classic textbooks are Denning (1983) and Koblitz (1994), and encyclopedic compendia include Schneier (1996) and Menezes *et al.* (1996).

Public key infrastructure (PKI) systems are one such encryption technology (Adams *et al.*, 2001; CCITT, 1988; Housley *et al.*, 2002; Polk, *et al.*, 2002). Important PKI-based secure protocols include the retail mechanism, Secure Socket Layer (SSL) (Dierks and Allen, 1999; Rescorla and Schiffman, 1995), and the interbank standard suite, ANSI X9 (American National Standards Institute, 1994; RSA Security, 2003a). The PKI is a flexible key distribution system in which every participant carries two cryptographic keys, one for encryption and one for decryption; together these two keys make up what is called an asymmetric *key pair* (Diffie and Hellman, 1976; Rivest *et al.*, 1978). The encrypting key is published to the world and is called the participant's *public key*. The decrypting key is called the *private key*. The system is characterized by mathematical elegance, efficient scaling features, and theoretically based security guarantees. A performance advantage of PKI is that it does not require a centralized, highly available intermediary for every secure transaction; however, this also makes it difficult to know when another party's key has been stolen or otherwise compromised. As such, PKI often requires a centralized, highly available intermediary for key management and especially for *prompt* notification about revoked key pairs (Adams and Farrell, 1999). This issue, the *revocation problem*, is still unsolved (Davis, 1996, 1998), despite the best effort to date (Myers *et al.*, 1999).

A digital signature (Rabin, 1978; Rivest *et al*., 1978) is *the* salient application of public key cryptography (and, by extension, of PKI) and is an analog of a handwritten signature. A digital signature is a cryptographic tag that only one author can calculate; the tag can be combined with any kind of data that the author might create (e.g., financial, entertainment, medical), and the tag's validity can be checked by anyone who can access the data. This combination of authored content with the author's identity serves the same purpose as applying one's signature to a paper document; a digital signature can be used to sign contracts, to provide authenticity of an electronic distribution, or to prove identity for access. Although e-commerce digital signatures have been much anticipated, they have been little adopted to date. There is still substantial research potential in understanding the legal and economic issues involved in the lack of widespread adoption of digital-signature-based electronic commerce.

In symmetric key systems, on the other hand, the same key is used for both encryption and decryption, so it must always be guarded as a secret. For e-commerce applications, the principal examples of symmetric key systems are the ciphers DES (NIST, 1993), AES (NIST, 2001), and RC4 (RSA Security, 2003b), as well as Microsoft's Hailstorm authentication system (formerly PassPort). As an advantage, symmetric key cryptography runs orders of magnitude faster than public key cryptography.

These ciphers can be used in a variety of ways. As noted earlier, the technical challenge in authenticating users is that the identifying information must remain private, but the Internet is a public broadcast medium. Cryptography meets this challenge by guaranteeing that the subscriber's identifying information cannot be stolen, copied, or replayed by others. It was once supposed that most users would use public key cryptography to authenticate themselves. However, very few end users possess public key certificates currently, because certificates are expensive. Instead, Web users use a variant of SSL in which users identify themselves with passwords instead of with digital signatures. A second way in which e-commerce sites validate users' passwords is with HTTP cookies. Cookie-mediated authentication, however, is very insecure (Dawson, 1998; Festa, 1998). Symmetric key cryptography offers more security than password-mediated authentication, with more favorable key management trade-offs than PKI affords, but as noted earlier the key must be tightly guarded.

Other technologies can be used to perform both authentication and data protection. For example, smart cards (Rankl and Effing, 1997) can be used to store data about the bearer of the card, including financial data, medical records, and identification credentials. Because those data are so sensitive, it is critical to store the associated encryption keys in tamper-resistant hardware. Further, the smart card should never have to share the bearer's per-

sonal data or her keys with a POS terminal, otherwise the bearer's privacy and keys could be compromised. In practice, this means putting a computer processor and cryptographic hardware on the card, along with the encryption keys. A further advantage is that smart cards can allow POS transactions to be more intricate, because all of the user's data are always available. This architecture can also avoid the centralized storage of personally sensitive data and supposedly demands less trust of the consumer to a centralized authority to husband the data properly. Smart cards have the disadvantage that every promise of tamperproof packaging has been shown to be false (Anderson and Kuhn, 1996, 1997). Smart cards saw early and widespread deployments in Europe, especially in Germany, Benelux, and France, but not in the United States. The reason for smart cards' adoption failure in the United States remains unclear.

Similarly, cryptographic technologies can be used at various points in the payment system (Neuman and Medvinsky, 1998). The majority of Web transactions are currently SSL-protected credit card transactions. However, many other mechanisms have been proposed for handling electronic payments. Digital cash and networked payments (e.g., Chaum, 1985) purport to bring anonymous electronic transactions to e-commerce; that is, like currency and unlike credit cards, digital cash cannot be traced to any specific individual. Thus, a consumer might buy electronic data or a digital service without revealing his identity to the merchant and without revealing his purchases to a financial clearinghouse. There are many digital cash variants, but Chaum's version was the archetype, using digital signatures and encryption to simulate the issuance of paper currency with serial numbers. In some variants, this currency can be given to others while not having the side effects of allowing counterfeiting, duplication, or double spending. Micropayment schemes, such as MilliCent (Glassman *et al*., 1995), are systems for transferring extremely small payments, perhaps fractions of cents, for Internet goods (often information goods). The goal in this case is to enable the creation of markets for small quantities of data and services, such as per-article newspaper subscriptions. Despite these interesting social and technical advantages, these sophisticated digital payments schemes have not thrived, for a variety of reasons. Shirkey (2000) has provided sharp arguments for why micropayments have not caught on: the history of communication markets shows that users greatly prefer simple and predictable pricing schemes. The Mondex anonymous payments system has been successful in Europe, but cryptographers have raised questions about Mondex's security (Brehl, 1997). Similarly, PayPal, a payment intermediary, has been financially successful but has been plagued by repeated problems with fraud (Jonas, 2002). Indeed, Stefan Brands, a cryptographer specializing in the design and analysis of digital cash systems, noted in 1996 that, of

the digital cash issued in European pilot deployments, 10% had been lost to fraud (Brands, 1996).

The entertainment and mass media industries have invested much effort in digital watermarking technology (Delaigle *et al*., 1996). Here, the technical goal is to find ways of cryptographically tagging electronic content (especially images and audio) so that it is recognizable, nonforgeable, and nonremovable. The business goal is to enable firms to detect unlicensed distribution or resale, in the hope of firms being able to distribute content electronically and safely. The watermark tag is generally designed to be invisible or unobtrusive. This is still an active area of research, as all proposals to date have been successfully attacked (Craver *et al*., 2001). Currently, the entertainment industry is using the Digital Millennium Copyright Act of 1998 (DMCA) to bolster with law the technical weaknesses of digital watermarking proposals, by making it illegal in the United States to remove or forge such protections (Lazowska, 2001).

C. Social and Organizational Issues in Security

Security, however, is not just a matter of technology; the implementation of technology without the proper organizational processes will not solve security problems (Treese and Stewart, 1998). There are a number of critical social and organizational issues with security. The first is that the weak link in security is often users or employees, rather than the technology per se (Anderson, 1994). The second is software engineering management, or managing how security technology is deployed (Anderson, 2001a). The third is the development of adequate organizational processes for risk management, separation of duties, development of security policies, access control, and security assurance.

A persistent problem is users' differing and incorrect models of security and their seeming inability or unwillingness to adhere to critical security policies and guidelines. Not only do users not understand what they need to do, but they often will not take the precautions necessary for the security technologies to work effectively (Davis, 1996). For example, users may store passwords in unencrypted files on vulnerable machines, or employees may divulge their passwords to third parties. The ability of hackers to obtain critical authenticity data is well-known; it is often called "social engineering" (Mitnick and Simon, 2002). Currently, this is an open research area. There is research on understanding users' mental models and motivations [e.g., Adams and Sasse (1999), Friedman *et al*. (2002)], but little on how to deal with the problem. We suggest that a networked application cannot offer full measures of connectivity, security, and ease-of-use, all at the same

time; there seems to be an intrinsic trade-off here, and some sacrifice is unavoidable. Until security vendors achieve the necessary delicate balance of all three desiderata, effective e-commerce security will remain a problem.

A second problem is that software management is a substantially larger problem with security than with many other types of software. As mentioned, hackers constantly discover new vulnerabilities in both new and existing systems. Standards and protocols are in a state of constant turmoil. Even keeping up to date with all security advisories and security patches is difficult, arguing that merchants should be conservative about undertaking complicated, heterogeneous deployments (Schneier, 2001). Indeed, because many merchants' e-commerce applications rely on client-side security features, it is important to remember that security holes tend to be very version-specific, making the software portability problem even worse. In addition, assessment of new security-relevant technologies is at once urgent and quite difficult. It is particularly hard to determine which technical proposals will succeed, but to be competitive and to avoid embarrassment, firms cannot afford to wait for standards to settle before beginning to build and deploy security solutions. Finally, in software management, security programmers are a limiting resource. There is currently a dearth of programmers who understand security. The software they write usually is subtle and hard to maintain, but naturally security specialists do not want to be boxed into dead-end software maintenance jobs. Thus, security products are often poorly maintained, with old security holes reappearing from time to time.

User and employee limitations as well as the chronic problems of software management suggest that organizations need to have a set of organizational processes in place to assess security vulnerabilities, manage their risk, and contain intrusions (Bishop, 2003; Treese and Stewart, 1998). [One is again referred to applied security publications, such as Garfinkel (2002) and Tipton and Krause (2002), for the details of specific policy and process recommendations.]

Organizational processes can offer important security protections. By creating a chain of responsibility and the proper separation of duty, organizations can be protected against intrusions as well as criminal insiders. Organizations must consider and insist upon policies for confidentiality of data, as well as the integrity of the data; that is, there must be policies in place to prevent both the leakage and the corruption of data (Bishop, 2003). Organizations must strive to create processes for determining access control to sensitive data, how intrusions or break-ins will be contained, and levels of risk (Tipton and Krause, 2002) and assurance. [See Bishop (2003) for a discussion of formal methods in security assurance.]

Without the necessary technologies and organizational processes in place, merchants stand to lose just as much as consumers, proportionally, if

an e-commerce deployment is insecure. Security breaches are newsworthy, and a merchant must be able to protect customers' identities, financial data, and shopping choices from exposure, so as to avoid alienating loyal customers.

Moreover, an underappreciated risk is that an insecure e-commerce server can undermine corporate regulatory compliance. In the United States, this risk is particularly important for financial systems, because securities laws require brokerages to keep extensive archives of internal communications and to prevent even insiders from accessing certain documents. An insecure e-commerce deployment can cause a financial institution to leak information in actionable ways, allow insiders to cover up misdeeds, or even allow insiders to generate falsified audit logs of nonexistent transactions.

D. Economic Issues

Again, an understanding of security would be incomplete without an analysis of the underlying economic issues. The preceding sections presented security either as a technical imperative or as a set of social and organizational issues; however, it must be stressed that security for both consumer and site requires an analysis with the proper weighing of potential risk. More importantly, as Anderson points out, security engineering is a matter of control and power, as well as access (Anderson, 1994, 2001b). Security mechanisms can be used to govern compatibility and attempt to control network effects governing the adoption of new or potentially replacing technologies (Shapiro and Varian, 1999). Indeed, Anderson argues that security technologies are often deployed as much for risk reassignment as risk reduction. An excellent collection of links to economics-based analyses of security is http://www.cl.cam.ac.uk/~rja14/econsec.html.

IV. CONCLUSION

In summary, privacy and security are still ongoing research problems. There have been some interesting and significant findings, however, in the past 5 years that bear important consequences for e-commerce sites and consumers. Privacy is now understood by many to be a social construction, with expectations being the largest consideration. Yet privacy is also considered a public issue by regulators, who have nonetheless largely allowed technology to unfold to date. Security is now understood to be largely imperfect, a continual cat-and-mouse game of security expert and hacker.

Important technical developments have been deployed in the past 5 years; however, it is clear that organizational policies may play as an important a role in site security. Finally, detailed economics-based and sociologically based analyses are beginning to find their way into the published literature, and we expect that these studies will bring greater clarity and proficiency to admittedly murky areas.

REFERENCES

Ackerman, M. S., and Cranor, L. (1999). Privacy Critics: UI Components to Safeguard Users' Privacy. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99)*, 258–259.

Ackerman, M. S., Darrell. T., and Weitzner, D. J. (2002). Privacy in Context. *Human–Computer Interaction* **16**(2–4):167–176.

Ackerman, M. S., Cranor, L., and Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce*, 1–8.

Adams, A., and Sasse, M. A. (1999). Users Are Not the Enemy. *Communications of the ACM* **42**(12):40–46.

Adams, C., and Farrell, S. (1999). Internet X.509 Public Key Infrastructure Certificate Management Protocols. Internet RFC 2510.

Adams, C., Sylvester, P., Zolotarev, M., and Zuccherato, R. (2001). Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols. Internet RFC 3029.

American National Standards Institute (1994). Accredited Standards Committee X9 Working Draft: Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman. ANSI X9.42-1993.

Anderson, R. (2001a). "Security Engineering: A Guide to Building Dependable Distributed Systems." New York: John Wiley & Sons.

Anderson, R. (2001b). Why Information Security is Hard—An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*.

Anderson, R. (1994). Why Cryptosystems Fail. *Communications of the ACM* **37**(11):32–40.

Anderson, R., and Kuhn, M. (1997). Low Cost Attacks on Tamper-resistant Devices. *Proceedings of the Security Protocols, 5th International Workshop*, 125–136.

Anderson, R., and Kuhn, M. (1996). Tamper Resistance—A Cautionary Note. *Proceedings of the Second USENIX Workshop on Electronic Commerce*, 1–11.

Bernard, H. R. (2000). "Social Research Methods: Qualitative and Quantitative Approaches." Newbury Park, CA: Sage.

Bishop, M. (2003). "Computer Security." New York: Addison-Wesley.

Borisov, N., Goldberg, I., and Wagner, D. (2001). Intercepting Mobile Communications: The Insecurity of 802.1. *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking*, 180–189.

Brands, S. (1996). "Electronic Cash." Invited talk, RSA Cryptographers' Colloquium.

Brehl, B. (1997). Security of "Cash Cards" Questioned. *Toronto Star* October 6, 1997, E1–2.

CCITT (1988). "Recommendation X.509: The Directory—Authentication Framework." Data Communications Network Directory, Recommendations X.500-X.521.

Chaum, D. (1985). Security Without Identification: Transaction Systems To Make Big Brother Obsolete. *Communications of the ACM* **28**:1030–1044.

Clarke, R. (2001). "Of Trustworthiness and Pets: What Lawyers Haven't Done for e-Business." http://www.anu.edu.au/people/Roger.Clarke/EC/PacRimCL01.html.

Clarke, R. (1999). "Introduction to Dataveillance and Information Privacy, and Definition of Terms." http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Cranor, L. F. (2002). "Web Privacy with P3P." Cambridge: O'Reilly & Associates.

Cranor, L., and Reagle, J. (1998). The Platform for Privacy Preferences. *Communications of the ACM* **42**(2):48–55.

Cranor, L. F., and Resnick, P. (2000). Protocols for automated negotiations with buyer anonymity and seller reputations. *Netnomics* **2**:1–23.

Craver, S., McGregor, J., Wu, M., Liu, B., Stubblefield, A., Swartzlander, B., Wallach, D., Dean, D., and Felten, E. (2001). "Reading Between the Lines: Lessons from the SDMI Challenge." Unpublished manuscript, to have been presented at the Fourth International Information Hiding Workshop, http://cryptome.org/sdmi-attack.htm.

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy and Marketing* **19**(1):20–26.

Culnan, M. J., and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science* **10**(1):104–115.

Davies, S. G. (1997). Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. *In* "Technology and Privacy: The New Landscape" (P. Agre and M. Rotenberg, Eds.), pp. 143–165. Cambridge, MA: MIT Press.

Davis, D. (1998). Non-linear Complexity of Revocation-checking. Post to the Cryptography Mailing List, Nov. 11, 1998, http://world.std.com/~dtd/compliance/revocation.html.

Davis, D. (1996). Compliance Defects in Public-Key Cryptography. *Proceedings of the 6th Usenix Security Symposium*, 171–178.

Dawson, K. (1998). JavaScript Privacy Bugs Hit Netscape, Then Microsoft. *Tasty Bits from the Technology Front*, October 12, 1998.

Delaigle, J.-F., De Vleeschouwer, C., and Macq, B. (1996). Digital Watermarking. *Proceedings of the Conference 2659—Optical Security and Counterfeit Deterrence Techniques*, 99–110.

Denning, D. (1983). "Cryptography and Data Security." New York: Addison-Wesley.

Dhillon, G. S., and Moores, T. T. (2001). Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal* **14**(4):33–37.

Dierks, T., and Allen, C. (1999). The Transport Layer Security Protocol. Internet RFC 2246.

Diffie, W., and Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory* **22**(6):644–654.

Etzioni, A. (1999). "The Limits of Privacy." New York: Basic Books.

Festa, P. (1998). Navigator Still Has Bug Problem. *CNet News.com*, October 7, 1998,

Fisher, S. (2001). Privacy By Design. *InfoWorld* **23**(27):20–22.

Fjetland, M. (2002). Global Commerce and the Privacy Clash. *Information Management Journal* **36**(1):54–58.

Friedman, B., Hurley, D., Howe, D. C., Felten, E., and Nissenbaum, H. (2002). Users' Conceptions of Web Security: A Comparative Study. *Proceedings of the ACM Conference on Human Factors and Computers (CHI'02)*, 746–747.

Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review* **52**:1461–1543.

Garfinkel, S. (2002). "Web Security, Privacy and Commerce." Cambridge, MA: O'Reilly and Associates.

Garfinkel, S., Schwartz, A., and Spafford, G. (2003). "Practical Unix Internet Security." Cambridge, MA: O'Reilley.

Glassman, S., Manasse, M., Abadi, M., Gauthier, P., and Sobalvarro, P. (1995). The MilliCent Protocol For Inexpensive Electronic Commerce. *Proceedings of the Fourth International World Wide Web Conference*.

Goffman, E. (1961). "The Presentation of Self in Everyday Life." New York: Anchor-Doubleday.

Graves, P., and Curtin, M. (2000). "Bank One Online Puts Customer Account Information At Risk." http://www.interhack.net/pubs/bankone-online.

Harris Poll (2000). Online Privacy: A Growing Threat. *Business Week*, March 20, 96.

Housley, R., Polk, W., Ford, W., and Solo, D. (2002). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet RFC 3280.

Jonas, J. (2002). "PayPal's Tenuous Situation." http://catless.ncl.ac.uk/Risks/21.92.html#subj6.

Koblitz, N. (1994). "A Course in Number Theory and Cryptography." Berlin: Springer-Verlag.

Lazowska, E. (2001). Overview of CRA and Felten *et al.*, http://lazowska.cs.washington.edu/felten/FeltenOverview.pdf.

Levy, S. (2001). "Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age." New York: Viking.

Light, D. A. (2001). Sure, You Can Trust Us. MIT Sloan Management Review **43**(1):17.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). "Handbook of Applied Cryptography." New York: CRC Press.

Mitnick, K. D., and Simon, W. L. (2002). "The Art of Deception: Controlling the Human Element of Security." New York: John Wiley and Sons.

Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (1999). X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP. Internet RFC 2560.

Neuman, B. C., and Medvinsky, G. (1998). Internet Payment Services. *In* "Internet Economics" (L. W. McKnight and J. P. Bailey, Eds.), pp. 401–416. Cambridge, MA: MIT Press.

Neyses, J. (2002). "Higher Education Security Alert From the U.S. Secret Service: List of Keystroke Logging Programs." http://www.unh.edu/tcs/reports/sshesa.html.

NIST (2001). "Advanced Encryption Standard (AES). FIPS PUB 197." http://csrc.nist.gov/encryption/aes/.

NIST (1993). "Data Encryption Standard. FIPS PUB 46-2." http://www.itl.nist.gov/fipspubs/fip46-2.htm.

P3P (2002). "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification." MIT/World Wide Web Consortium. http://www.w3.org/TR/P3P/.

Polk, W., Housley, R., and Bassham, L. (2002). Algorithms and Identifiers For the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet RFC 3279.

Rabin, M. O. (1978). Digitalized Signatures. *In* "Foundations of Secure Computation." (R. Lipton and R. De Millo, Eds.), pp. 155–166. New York: Academic Press.

Rankl, W., and Effing, W. (1997). "The Smartcard Handbook." New York: John Wiley.

Reidenberg, J. R. (1999). Restoring Americans' Privacy in Electronic Commerce. *Berkeley Technology Law Journal* **14**(2):771–792.

Rescorla, E., and Schiffman, A. (1995). "The Secure HyperText Transfer Protocol." Internet Draft, version 1.1.

Rivest, R., Shamir, A., and Adelman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* **21**(2):120–126.

Roberts, P. (2002). Bugbear Virus Spreading Rapidly. *PC World Online*, Ocotober 2, 2002.

RSA Security (2003a). "What Are ANSI X9 Standards?" Cryptography FAQ, http://www.rsasecurity.com/rsalabs/faq/5-3-1.html.

RSA Security (2003b). "What Is RC4?" Cryptography FAQ, http://www.rsasecurity.com/rsalabs/faq/3-6-3.html.

Schneier, B. (2001). The Security Patch Treadmill. *Crypto-Gram Newsletter*, March 15, 2001, http://www.counterpane.com/crypto-gram-0103.html#1.

Schneier, B. (1996). "Applied Cryptography." New York: John Wiley & Sons.

Shapiro, C., and Varian, H. R. (1999). "Information Rules." Cambridge, MA: Harvard Business School Press.

Shirkey, C. (2000). "The Case Against Micropayments." O'Reilly OpenP2P.com, Dec. 19, 2000, http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 167–196.

Spiekermann, S., Grossklags, J., and Berendt, B. (2001). E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. *Proceedings of the ACM Conference on Electronic Commerce*, 38–46.

Tipton, H., and Krause, M. (2002). "Information Security Management Handbook." New York: CRC Press.

Treese, G. W., and Stewart, L. C. (1998). "Designing Systems For Internet Commerce." New York: Addison-Wesley.

Westin, A. F. (1991). "Harris-Equifax Consumer Privacy Survey 1991." Atlanta: Equifax, Inc.

Winner, D. (2002). Making Your Network Safe for Databases. *SANS Information Security Reading Room*, July 21, 2002.