The Privacy Gap: Managing Website Privacy
Privacy challenges stem from eBusiness

The emergence of the Internet and the World Wide Web has provided an unprecedented ability for people to conduct electronic business. However, this real-time connectivity has resulted in significant threats to individual privacy. The same mechanisms that underpin the power of the Web can also be used, sometimes without the user’s knowledge or consent, to collect sensitive information about an individual or their Internet usage behavior.

Powerful data collection techniques, users’ inability to know what is being collected or how to stop it, combined with media exposure of perceived ‘bad actors’ in privacy, have resulted in an increasing lack of trust among web users. In turn, this lack of trust translates into lost revenue.

The fundamental concept of trust underpins business relationships

What exactly is trust? Trust is the foundation of a relationship between a customer and an organization. Trust decreases feelings of insecurity, binds people together, and enables confidence. Over time, trust grows as organizations behave consistently and predictably. The result is faith in an organization’s ability to conduct business with integrity, which in turn translates into more profitable business transactions.

Build trust in the online economy by proactively managing privacy challenges

In the old economy, organizations and users chose to interact with each other based on trust. In the new economy, the concept of trust is still evolving but it will play an instrumental role in the success of e-business initiatives. Trust will be built when users have a successful online experience with an organization. Additionally, trust will come from an organization’s respect of a customer’s privacy.

The level of trust will continue to grow with each successful and positive online interaction. It can even become a competitive advantage. If users trust an organization more than its competitors, they are likely to select the trustworthy organization over its competitors. In turn, this translates into stronger market share and increased revenue.

However, trust is not earned over night. Rather the establishment of trust between a customer and an organization needs to evolve over time. Therefore, it is critical for companies to act now and establish formal website privacy policies and proactively monitor their actual practices – before a website privacy breach occurs. By acting now, organizations can build their credibility and earn consumer confidence.

Organizations need to build online trust now

New ebusiness enabling technologies such as wireless technology will give rise to even more privacy concerns because of the ability for organizations to do more targeted profiling and location based targeting. In such times, users will turn to those organizations with a proven track record of respecting users’ privacy. By acting now, organizations can build their credibility and build a strong foundation of trust.

Only by building and maintaining their users’ trust, can companies build profitable online relationships with their users. Only then can organizations truly maximize the opportunities afforded by e-business.

-- Steve Del Vecchio, Partner and ebusiness Solutions Leader, PricewaterhouseCoopers
# Table of Contents

INTRODUCTION............................................................................................................. 1

SERIES OVERVIEW............................................................................................................ 2

WHAT’S CAUSED THE PRIVACY GAP......................................................................... 3

INCREASED PERSONALIZATION OF SITE CONTENT ......................................................... 3

MEDIA EXPOSURE OF LACK OF ONLINE PRIVACY PROTECTION............................... 3

GLOBAL FLOW OF INTERNET INFORMATION ............................................................... 3

CURRENT METHOD OF WEBSITE PRIVACY MANAGEMENT ........................................... 4

WHAT PRIVACY NON-COMPLIANCE MEANS TO YOU................................................... 4

Worldwide legislation........................................................................................................ 5

Class-action lawsuits.......................................................................................................... 7

Lost business.................................................................................................................... 7

Brand and reputation erosion.......................................................................................... 7

WHAT ARE THE PRIVACY RISKS? ............................................................................... 8

Privacy statements............................................................................................................ 8

Web forms....................................................................................................................... 9

Cookies......................................................................................................................... 10

Web beacons.................................................................................................................. 10

Third party links............................................................................................................. 10

Integrated third party content........................................................................................ 10

CLOSING THE PRIVACY GAP ..................................................................................... 11

MAINTAINING COMPLIANCE NOW AND GOING FORWARD ...................................... 11

Create and maintain a privacy risk management checklist............................................. 11

Adhere to privacy policies............................................................................................... 12

Understand worldwide privacy legislation...................................................................... 13

Establish the role of the Chief Privacy Officer............................................................... 14

Include privacy seals....................................................................................................... 14

Automate website privacy management.......................................................................... 15

CONCLUSION............................................................................................................... 17

Benefits of good privacy practices.................................................................................. 17

THIS WHITE PAPER WAS BROUGHT TO YOU BY ......................................................... 18

OTHER PRIVACY LINKS ............................................................................................... 18

WHAT’S NEXT? .............................................................................................................. 18

Worldwide Locations:

1 Hines Road, Kanata, Ontario K2K 3C7  Tel +1 613 599-3888  Fax +1 613 599-4661
1 Cranberry Hill, Lexington, Massachusetts, USA  02421  Tel 1-800-282-5951 Tel +1 781 372-5900 Fax +1 781 274-8706
Royal Albert House, Sheet Street, Windsor, Berkshire, United Kingdom SL4 1BE Tel +44 (0) 1753 705 010 Fax +44 (0)
1753 705 019

© Copyright 2001 Watchfire Corporation. All Rights Reserved. Watchfire, Watchfire Enterprise Solution, Linkbot, Macrobot, Metabot, Watchbot,
WebCPO and the flame logo are trademarks or registered trademarks of Watchfire Corporation. All other products, company names and logos are
trademarks or registered trademarks of their respective owners.
Introduction

The emergence of the Internet and the World Wide Web have provided an unprecedented ability for people to both access and publish information interactively. The main benefits of the Internet — high visibility and readily accessible information — clash with the basic premise of personal privacy. However, corporations strive to reconcile the two if they want to maximize the opportunities afforded by the Internet. B2Cs (business to consumer) must ensure that they protect consumers, who have a right to know how their personal information is being collected, used, and shared. B2Bs (business to business) must ensure they protect sensitive business information to maintain partner relationships.

Websites collect and track consumer, employee, and business information through the use of online forms, and technologies such as server logs, cookies, and web beacons. Powerful data collection techniques and users’ inability to know what is being collected or how to stop it, combined with media exposure of perceived ‘bad actors’ in privacy, have resulted in an increasing lack of trust among web users. To properly notify web users, corporations must post privacy statements so that visitors can make informed decisions about how they want to interact with a website. Most importantly though, corporations must ensure that once they develop these privacy policies, they adhere to them. The risks of failing to be privacy compliant are simply too high.

Privacy breaches can happen anywhere on your Web properties: your employee intranet, your partner/supplier extranet, and your corporate website. No site or market is immune from potential privacy glitches: they happen on both B2C and B2B sites. While online privacy breaches most definitely affect consumers, the organizations making these transgressions hardly go unaffected. The repercussions of privacy glitches can be significant: lost revenue and business opportunities; brand and reputation erosion; adverse media attention; unwanted scrutiny from consumer advocates; class-action lawsuits; and legislative penalty. While website privacy management is just one aspect of your privacy compliance strategy, ignoring your website’s privacy management practices is risky.

In Setting the Scene for Website Management, the first paper in the Bad Things Shouldn’t Happen to Good Websites™ series, we introduced the concept of the ‘Web Experience Gap’, the difference between what users expect from websites and what websites actually deliver. Co-authored with PricewaterhouseCoopers, this white paper explores the ‘Privacy Gap’, the difference between what privacy protection users expect from websites, and what privacy protection websites actually offer, and what the business implications are of non-compliance. We’ll examine how the privacy gap is part of the overall Web Experience Gap users are facing. Lastly, we’ll offer suggestions on what you can do to better manage your website privacy and help avoid potential privacy issues.

PricewaterhouseCoopers — the leading provider of privacy consulting and assurance services— and Watchfire Corporation— the leading provider of Website Management software and services— have formed an alliance to provide a powerful Website Privacy Management solution for enterprise websites. This alliance leverages PricewaterhouseCoopers’ experience in offering its clients a full range of privacy risk-management and compliance programs, and Watchfire’s depth of expertise in developing enterprise solutions for analyzing websites. The benefits of using this co-developed website Privacy Management Solution will be discussed later in the white paper.
Series Overview

You’ve worked hard to create the best possible web experience. So bad things shouldn’t be happening to your website … but they are.

Right now your website probably has problems that limit the success of a visitor’s experience. Because of this, Watchfire has brought together an unparalleled team of industry and technology partners to develop a comprehensive resource for web stakeholders —the Watchfire *Bad Things Shouldn’t Happen to Good Websites™* White Paper Series.

Whatever your role (Chief Privacy Officer, eBusiness Manager, Web Master, Producer, Developer, QA Manager/Director of IT, Director of Visitor Experience), this indispensable series covers the business issues, industry statistics, and technical solutions relevant to you, including topics such as:

- Content Delivery
- Website Accessibility
- Website Privacy
- Content Management
- E-Intelligence
- Searchability
- Performance Management
- User feedback

This series looks at website problems, how they affect business, and how to fix them. It will explore how a variety of complementary services and solutions from Watchfire technology and service partners fit together with Website Management to help bridge the Web Experience Gap.
What’s Caused the Privacy Gap

On the Internet, information, commerce, and communications flow freely across national borders. The Internet’s decentralized, open, and interactive characteristics have accelerated the trend toward increased information collection, use and sharing. Because the Internet information and commerce market is global, organizations must consider how the laws regulating business and issues arising from privacy breaches around the world will affect them.

Increased personalization of site content
Personalization, the very innovation that has lead to target marketing, can in fact, lead to privacy issues. Many companies offer consumers website content that’s personalized and relevant to them in the hopes of increasing sales, improving services, strengthening relationships, facilitating site use, and helping retain customers. Consumer requests for heightened customer service also requires the continued collection of personal information. To enable these efforts, companies collect customer names, email addresses, age and gender, and even credit card information via online forms. In addition, many websites personalize the content based on a user’s preferences or behavior, which is tracked through technologies such as server logs, cookies, and web beacons. But the manner in which businesses collect information about consumers is at the root of the privacy problem: how much information should they collect, how much should they use, and how much, if any, should they share with other vendors and partners?

Media exposure of lack of online privacy protection
Major hurdles to consumer participation in electronic commerce are the countless surveys detailing the lack of online privacy protections. In a Business Week Privacy Survey/Harris Poll, 63% of Internet users claimed they would not be comfortable with websites tracking their movements, even if the websites did not tie any information to the individual. 89% of Internet users claimed they weren’t very comfortable at all with websites merging their browsing and shopping habits with their real world identities1. While generally admitting that they are happy to receive offers and content of special interest, consumers often become extremely worried at the privacy implications of personalization. This concern is heightened when they receive personalized communication from an unknown third party with whom they have had no previous contact.2

Global flow of Internet information
Another contributor to the Privacy Gap is that information on the Internet flows effortlessly from country to country, organization to organization, and government jurisdiction to government jurisdiction. Governments around the globe are struggling with how to develop appropriate and effective privacy rules and regulations. Even so, each country approaches and handles privacy differently. The United States, for example, tends to favor a looser self-regulatory approach; Europe favors wide-ranging data protection legislation. Under the glare of public, regulatory and legislative scrutiny, a growing number of organizations have started to incorporate privacy compliance into their management process.

---

1 Business Week Privacy Survey/The Harris Poll, Harris Interactive Inc., 2000
Current method of website privacy management

Websites are too complex for manual checking. Contributing to the privacy gap is the fact that the task of manually managing website privacy compliance can be difficult and costly. The size and scope of enterprise websites makes manually checking for privacy issues a challenge and the task of ongoing privacy compliance a burden – there are too many privacy issues to look for spread across thousands, if not millions, of pages to effectively guard against potential privacy breaches.

Websites are large and constantly changing; most sites are adding new content every day to thousands, if not millions, of pages. These sites bring new challenges and measurement requirements to organizations trying to ensure their websites are privacy compliant. Managing website privacy is not a one-time event. Every time content and transaction functionality is added or changed, there is an inherent risk of exposing your site to privacy risks and non-compliance.

Executives at many large companies are frequently unfamiliar with the extent of their own information-gathering practices. Many organizations assume their web teams know about their privacy policies. Still others are not aware of what kind of information their websites collect. This lack of formal website privacy management practices and the reliance on manual spot checks to manage potential privacy issues is costly and inefficient, not to mention risky. There are simply too many issues to look for spread across the website, resulting in a lack of control over an organization’s privacy practices and guidelines. This can leave the organization vulnerable, making it reactive, rather than proactive, to privacy breaches.

What privacy non-compliance means to you

Issues relating to privacy on the Web are resulting in widespread market backlash such as lost revenue and business opportunities; brand and reputation erosion; adverse media attention; unwanted scrutiny from consumer advocates; class-action lawsuits; and new and sweeping worldwide legislation. Consumers, businesses, and employees are becoming increasingly aware of privacy issues as they relate to the Internet and many will not conduct business on websites without privacy statements or assurances. Consider these statistics from recent Privacy Exchange Organization and Harris-Westin Consumer surveys:

- 80% of Americans feel consumers have lost control over how personal information is circulated;
- 90% of Net users and purchasers want websites to post notices explaining how personal information is used

The cost of mismanaging privacy can be loss of revenue, adverse publicity, reputational damage and legal action.
People first flocked to online commerce for its convenience, but consumers have drawn away – 60 percent now abandon their online shopping carts before completing the purchase. According to IDC, many shoppers attribute their flight to privacy concerns. A similar scenario is occurring in Europe: a 1999 Jupiter survey of European online retailers found security and lack of trust to be rated among the greatest barriers to growth for online commerce in Europe. Recent American surveys from IDC support Jupiter’s European findings: 9 out of 10 American Web users have not made an online purchase in the last six months.

**Worldwide legislation**

In addition to consumers’ concerns, there has been new and sweeping worldwide legislation. Businesses must identify and stop online privacy breaches to ensure legislative and industry compliance. Most of the laws being passed incorporate rules that govern the collection, use, retention, and distribution of personal data. Determining how to handle variations in legislative requirements, while accommodating the various industry regulatory practices to privacy, becomes a compliance risk management decision. Because at least 50 countries around the world have different privacy laws, (some more stringent than others), global compliance for an organization requires the creation of a baseline of privacy protection. Organizations must determine how they should operate with respect to this baseline, particularly those that operate internationally, since they must comply with requirements from the European Union, Canada and other entities. Even within the United States, there are myriad privacy laws and regulations between states and the federal jurisdiction.

**US legislation**

**Gramm-Leach-Bliley Act of 1999:** The US Federal Trade Commission recently finalized its rules for implementing the Gramm-Leach-Bliley Act, which became effective November 13, 2000, with full compliance required by July 2001. It regulates the privacy of personally identifiable, non-public financial information disclosed by financial institutions to non-affiliated third parties for the purposes of telemarketing or other direct marketing. The law requires that consumers be given notice, an opt-out choice, and reasonable security for their financial data. It prohibits the disclosure of account numbers and access codes for credit, deposit or transaction accounts to a non-affiliated party for marketing purposes. The GLBA also requires financial institutions to notify customers of their privacy policies and practices.

**Health Insurance Portability and Accountability Act (HIPAA) of 1996:** The US department of Health and Human Services is finalizing privacy rules directed by the HIPAA. These regulations, which go into effect in 2003, will standardize the sharing of medical information by doctors, hospitals, insurers, and health care clearinghouses. It requires all covered entities to obtain patients’ opt-in via consent forms for any use and disclosure of protected information for treatment, payment or health care operations. Health care providers must provide written notice of how protected health information about an individual will be used, as well as an accounting of the circumstances surrounding certain disclosures of the information.

**Children’s Online Privacy Protection Act of 1998:** Enacted into law in 1998, COPPA requires that websites that are visited by children under the age of 13 post a privacy policy detailing any personally identifiable information collected from those children. Sites also must obtain verifiable parental consent before collecting, using, or disclosing personal information from children under the age of 13.

---

**European legislation**

The EU Directive, which went into effect in October 1998, requires all EU member states to pass legislation meeting the standard set by the Directive. The laws of each country must address specific requirements around data quality, processing of sensitive data, notice given to data subjects, the right to access personal data, security requirements, and enforcement. The intent of the Directive is to harmonize laws throughout the EU and ensure consistent levels of protection for all citizens, as well as allowing for the free flow of personal information throughout the EU. The EU Directive limits the nature of data transfers to countries like the United States that do not have “adequate” data protection legislation (as determined by the EU). In response to this restriction, the US Department of Commerce and the EU recently agreed to the Safe Harbor Principles, which are standards that US companies can meet in order to continue transferring data to and from Europe.

**Canadian legislation**

**Personal Information Protection and Electronic Documents Act (Bill C6):** This law became effective January 1, 2001, and sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to see and ask for corrections to information an organization may have collected about them. The Act applies to personal information about customers or employees that is collected, used or disclosed by the federally regulated sector in the course of commercial activities. Foreign companies doing business in Canada will also be subject to the Act for activities conducted in Canada. Personal health information collected, used or disclosed by these organizations will not be covered until January 1, 2002. The Act will come into full effect on January 1, 2004, at which time it will apply to all intra-provincial, inter-provincial and international commercial activities of all organizations.

**Legislative penalty**

Some of the existing and proposed privacy and data protection law around the globe can result in financial penalty and even prison sentences for non-compliance. The following table illustrates various US laws related to consumer trust and the maximum civil penalties per infringement associated with them.

<table>
<thead>
<tr>
<th>Area</th>
<th>Regulatory Agency</th>
<th>Data Collection</th>
<th>Third-Party Disclosure</th>
<th>Maximum Civil Penalty</th>
<th>Right of Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>COPPA</td>
<td>Children FTC</td>
<td>Opt-in†</td>
<td>Opt-in</td>
<td>$11,000</td>
<td>Federal</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Care Health and Human Services</td>
<td>Opt-out</td>
<td>Opt-in††</td>
<td>$250,000</td>
<td>Private</td>
</tr>
<tr>
<td>GLB</td>
<td>Financial OCC, FTC, SEC, FRB, FDIC, NCUA, OTS, and state insurance regulator</td>
<td>Opt-out</td>
<td>Opt-out</td>
<td>$11,000</td>
<td>Federal</td>
</tr>
<tr>
<td>F CRA</td>
<td>Financial Institutions FTC</td>
<td>N/A</td>
<td>Opt-in</td>
<td>$2,500</td>
<td>Federal</td>
</tr>
</tbody>
</table>

† Consent is not required when site is collecting e-mail to provide notice or ensure safety.
†† De-identified data may be used freely.

Source: Jupiter Research
© 2001 Jupiter Media Metrix, Inc.
Class-action lawsuits

In January 2000, a number of class-action lawsuits were filed, and there appears to be a growing trend toward litigation surrounding online privacy breaches. These class-action privacy suits are extremely costly, both in terms of reputation and financial penalty. New class-action lawsuits brought against two Internet ad agencies claimed that the companies used cookies to track ad viewers’ online activities without their permission. In addition to targeting cookies, the plaintiffs alleged that the defendants used web beacons to identify individuals who visited sites that were part of the companies’ ad networks. The suits, which are still pending, could subject these companies to millions of dollars in damages.

In March 2000, it was discovered that one organization’s website was inadvertently transmitting personal financial information to an Internet advertiser. A number of related lawsuits resulted. In response to media inquiries about the practice, company officials said they were unaware of the problem. This experience highlights the difficulty of keeping track of all your website’s practices.

Lost business

According to a recent news report citing Forrester Research, 35 million Americans last year spent about $45 billion shopping online. But consumers would have spent an additional $12.4 billion if they hadn’t been concerned about the consequences of giving out personal data on the Web. Jupiter Communications has projected that privacy issues could potentially put an $18 billion dent in the $40 billion e-commerce revenue it projects by 2002.

Brand and reputation erosion

The cost of a privacy ‘glitch’ can range from tens of thousands to millions of dollars based on the company’s size and the visibility of its brand, warns Forrester Research, and this doesn’t include lost business and damage to the brand. John McCarthy, group director at Forrester Research, estimates that a small company might pay $44,000, including public relations costs, management time, customer service and outside consultants, to cope with a controversy about its use of personal information. At a large company, the cost could exceed $1 million.

The brand erosion and media attention arising from privacy breaches can be unwanted and irreparable; consider these examples:

- In November 2000, a hacker broke into an online auction site, potentially exposing its 3.7 million customer accounts. Weeks later, the company said the hacker didn’t gain access to any of the credit card numbers it had on file, but the brand erosion was already done; by then many of the credit cards had been canceled by banks or worried customers.

---

5 “Up for sale: Privacy on the Net”, CNET.com, March 25, 2001
6 “Industry Privacy Failures Hurting Ecommerce”, Privacytimes.com, September 1999
An online travel firm garnered over 20 media stories about its recent exposure of customer data when it made routine changes in its website infrastructure when some of the company's internal data from two promotional contests that ran last year was inadvertently left on a computer that is now being used as a Web server.

An online toy store came under fire from public critics in September 2000 because of an agreement with an analytics firm for visitor activity analysis. Class-action lawsuits were launched, alleging the toy store was selling personal information. Both companies contend that the data belonged to the toy store who sent it to the analytics firm to be compiled, and that the information was never sold. However, the perception of possible wrongdoing resulted in 12 major media stories and eventual termination of the relationship.

What are the privacy risks?
Privacy breaches can happen on many pages of your website and through a variety of different data collection technologies. The following diagram illustrates where your website may be unintentionally posing privacy risks.

Privacy statements
Privacy leaks can also occur through inadequate and un-enforced privacy statements. Many websites display a privacy statement explaining what the organization does with the information it collects from users. Other organizations require that every page that collects information from users include a link to the privacy statement. However, a privacy statement is only effective if it properly discloses and appropriately enforces an organization’s information practices and corporate privacy standards. A recent news item revealed that a popular Internet Service Provider (ISP) is modifying its future advertising to clarify that its members are not protected by its privacy policy when they surf sites that aren’t affiliated with the online service. The ISP made the change after the Better Business Bureau’s National Advertising Division raised concerns about the tagline, "At [ISP], your security and privacy are always protected."
**Web forms**

Fair information practices prescribe that users be informed of an organization’s information handling practices at the point at which personal information is collected. Many industry organizations also require that users be informed of an organization’s practices when personal information is collected. As such, many organizations have made it a policy to provide a link to their privacy statement on every web page with data collection forms.

Web forms are an area that can pose serious privacy problems on your website. Information is often collected from web users both with and without their knowledge when they submit data through forms. When the source page is delivered in response to a page or form that uses the “GET” method, certain information (including data that the end user entered into the form) may be inadvertently transmitted to the receiving server. Litigation and adverse publicity has resulted from the use of the GET method, therefore organizations should review their site to verify that they are not inadvertently transmitting personal user data to third parties.

**Cookies**

Cookies are small text files that are placed by a web server on an Internet user’s computer and act as digital identifiers. Most often, cookies are used to recognize a unique user during a particular visit to a website or to recognize the users when they subsequently return to a website. Privacy issues arise when 3rd party, persistent cookies are used to track a user’s movements throughout a website or across a network of websites. This ‘clickstream’ data can be used to build behavioral profiles of Internet users and enable companies to place targeted content on web pages based on an individual’s perceived preferences.

Some of the controversy surrounding cookies relates to situations where the identity of the user is disclosed and merged with the clickstream intelligence previously gathered. Privacy advocates and class-action lawyers have argued that this use of cookie technology constitutes a form of surveillance (akin to wire tapping) that monitors and stalks users without their knowledge. Generally accepted industry standards recommend that companies disclose their practice of online profiling by third party ad servers in their privacy statements and provide users with the ability to opt out of receiving third party cookies. Online consumers may be more willing to interact with a website if they are made aware of their choices, and the company’s practices as they pertain to the use of cookies.

**Web beacons**

Web beacons, also known as ‘web bugs’, ‘pixel tags’ or ‘clear gifs’, are small invisible graphic images that work in conjunction with cookies to count page visits, track movements and build behavioral profiles. They are inserted in the software code of websites and commercial emails to enable the provider to monitor who is reading the page or message in question. In recent years, website collection of information from Internet users without their knowledge has garnered media scrutiny and legislative attention. The use of web beacons has been especially criticized. As such, their use on your website imposes privacy considerations of which you should be aware.

Web beacons are considered controversial because, unlike cookies which can be detected and blocked by many popular Web browsers, web beacons are invisible and monitor online users without their knowledge. As a result, companies that choose to use web beacons should disclose the use of this technology in their privacy policies. Best practices advocate against using web beacons on “sensitive” sites, such as those sites that are financial or health-related.
Third party links

Managing your company’s data practices may encompass a due diligence of any third parties’ links on your website. Privacy concerns arise when links to external domains lead to third-party information sharing, especially if these external domains have privacy practices that differ from your own. Your organization may bear reputation and litigation risks if a linked site has questionable privacy practices. Identifying the linked sites can help you monitor and assess these risks.

Companies should strive to assure that parties with whom they have a business relationship have adequate security and privacy policies in place. If these third parties have substandard privacy practices, an organization may want to remove the links to these sites in order to avoid privacy risks. Understanding your business affiliates’ practices is just as important as knowing your own.

Integrated third party content

Additional privacy challenges are posed with the increasing amount of personalization of website content and integration of content by service providers and business partners. It is often not clear to the website visitor that a portion of the page or site is provided by a third-party organization and that the associated data collection is governed by a different privacy policy. Reputation is on the line, so careful review of these practices across the entire website infrastructure combined with an appropriate level of due diligence of the third parties is crucial to being comfortable.
Closing the Privacy Gap

According to the 12th annual Information Systems and E-Business Spending study conducted by Computer Economics, about one-third of all organizations have implemented a formal privacy plan. "By the end of 2002, over 50 percent of all organizations will have formalized a privacy policy," said Michael Erbschloe, vice president of research at Computer Economics and co-author of Net Privacy: A Guide to Developing & Implementing an Ironclad Ebusiness Privacy Plan. "Overall, things look good on the privacy planning front," said Erbschloe. "It is, however, rather alarming that there are so many organizations that have not started to formally address the need for managing privacy." The study found that 23.5 percent of organizations have not even begun developing privacy policies and plans.8 Computer Economics followed up with survey respondents to determine why this figure was so high; the majority said they do not know what to do or where to start, so they have not done anything.

Building trust can go a long way in convincing consumers to spend online. Effective, proactive, and cost-efficient privacy management can minimize the risk of regulatory investigation, class-action lawsuits, and legislative enforcement, and enhance the trust and confidence of your customers and partners.

Trust is the foundation of a sustainable relationship between the web user and the company. Violate this trust, and it's difficult and costly to re-establish. Therefore, it's critical for companies to establish formal website privacy policies and proactively monitor actual practices – to help avoid website privacy breaches. Only by building and maintaining their users' trust, can companies truly maximize the opportunities afforded by the Internet.

Maintaining compliance now and going forward

Create and maintain a privacy risk management checklist

In order to avoid costly website privacy breaches, it is recommended that companies create an ongoing privacy management program. The following are some general steps to take in such a program:

1. Create internal cross-functional privacy council or team – bringing together legal, marketing, HR, technology and internal audit expertise.
2. Understand privacy legislation and applicable industry-specific rules.
3. Create a mapping of all consumer collection and usage across all channels.
4. Assess relationships with third-party vendors and business partners.
5. Prepare official privacy policy that clearly describes the information handling practices to consumers and website users.
6. Ensure that adequate processes and controls are in place to demonstrate compliance with the privacy policy.
7. Conduct ongoing monitoring of compliance with the privacy policy.

8 "Only One-Third of US Firms have Privacy Plans", Newsbytes.com, May 9, 2001.
In addition, consulting firms such as PricewaterhouseCoopers help businesses manage their privacy risks throughout the organization by conducting regular privacy audits. Their services cover the following:

- **Privacy Policy**: Designing privacy policies for corporate and online business environments to meet the requirements of your strategic business needs and online privacy seal programs, and to ensure compliance with known local and international best practices and relevant regulatory or legislative requirements.

- **Compliance Programs**: Assisting organizations to develop internal frameworks and programs to monitor ongoing compliance with their privacy policies and reduce the risks of potentially damaging breaches inviting regulatory oversight actions.

- **Operational Procedures**: Developing or reviewing operational procedures within an organisation to ensure detailed procedural support for organization-wide privacy compliance.

- **Systems Security**: Assisting organizations to implement platform based, application and web security measures to address privacy considerations over data and transactions.

- **Readiness Reviews**: Assisting organizations preparing for new and evolving compliance requirements such as web-seal programs, as well as new industry codes, and regulatory or legislative requirements. This may include self-assessments, consulting services on targeted new companies or technology issues and gap analyses.

- **Privacy Audit**: Completing comprehensive assurance services, tailored to an organization’s strategic needs or consumer concerns, providing independent verification of compliance with privacy policies, privacy web-seal programs, or regulatory requirements.

- **Training and Awareness**: Providing tailored training to organizations and industries with regard to privacy-sensitive activities and implementing industry codes of practice and legislation.

- **Compliance Monitoring Tools**: Implementing software solutions that allow organizations to quickly monitor and regulate their privacy compliance. PricewaterhouseCoopers can develop customized electronic compliance checklists and assist in the rollout processes.

**Adhere to privacy policies**

In the US, an investment firm failed to adhere to its posted privacy policy and had to pay $4 million in fines. Ultimately, a company’s fear of a privacy breach might be the best incentive to be strict about privacy policies. "At this stage of the game, having a clearly communicated and easily understood privacy policy in place is a competitive advantage," says Chris Ferneyhough, Vice President of Technology Research at Ipsos-Reid. "Firms that have recognized this are enjoying..."
the benefit of being able to develop a better understanding of their current and potential online customers. Organizations that have not yet recognized the importance of a clear privacy policy are shooting themselves in the foot and are hindering their efforts to build strong and long-lasting online customer relationships.

Privacy policies have been posted on B2C websites as demonstrations of an organization’s privacy position, but they are often confusing, changeable, or out of date. Most B2B companies protect their privacy with contracts, non-disclosure agreements and other intellectual property protections. But their actual privacy practices are inconsistent; some companies rely on the trust established from long-term relationships. Others rely on a good track record; still others are hiring risk management companies to perform privacy audits on their websites.

“The first step toward a good privacy strategy is a good privacy policy,” says Chris Pickering, a senior consultant with the Cutter Consortium, an information technology consulting company. “And I believe both partners are responsible for privacy.” But the Cutter Consortium found that a large percentage of the 134 B2B and B2C businesses it surveyed recently had no privacy policy. Of those surveyed, 53% have a formal privacy policy in place — 47% do not. “There is plenty of cause for concern about that 47% with no privacy policy,” says Pickering. “The survey suggests that most companies are simply avoiding the issue by restricting the use of e-business-gathered data to internal use only.”

**Understand worldwide privacy legislation**

Adhering to new privacy legislation is quickly becoming a top concern for companies around the globe. Businesses must identify and stop online privacy breaches to ensure legislative and industry compliance. Some key pieces of legislation worldwide are:

- The Gramm-Leach-Bliley Act of 1999, (US) enforceable as of July 2001, restricts 3rd party data sharing. Business websites must provide notice and opt-out options prior to sharing information with non-affiliated 3rd parties
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (US), with the final rules recently approved by the Bush administration, requires companies that are collecting/transmitting health information to provide privacy protections. They must also establish a company official responsible for privacy compliance (i.e. Chief Privacy Officer).
- The Children’s Online Privacy Protection Act of 1998 (US) safeguards the collection and use of personal information from children under the age of 13 – requiring parental consent for any such activity.
- Personal Information Protection and Electronic Documents Act (Bill C6) — This Canadian law became effective on January 1st, 2001, and applies to the collection, use, and sharing of information on all federally regulated companies. Websites must obtain consent from consumers before collected information is used commercially.

---

Establish the role of the Chief Privacy Officer

It’s not enough to merely post privacy policies on a company bulletin board or at the company website. The direction and management of privacy has to be established and supervised by the very top management of the company. A new position has emerged among privacy-conscious organizations, particularly those that operate globally: the Chief Privacy Officer (CPO). CPOs address the new privacy needs by assessing risks, managing implementation of privacy policies and associated procedures, ensuring ongoing compliance, monitoring developments, accommodating changes, raising awareness in the organization, and training staff.

As companies grapple with new regulatory requirements, increased consumer and governmental scrutiny, and the realization that privacy will play a role in differentiating them from their competitors, increased emphasis is being placed on this new role. The majority of companies choose to locate the CPO in the Legal Department because initiatives under the governing authority of the Legal Department are usually taken seriously. Another advantage is that a significant amount of interpretation is required to understand the implications of a privacy policy on organizational procedures and potential litigation. Given the limited amount of case law available for the interpretation of new privacy laws, regulations, and self-regulatory standards, many companies need the expertise and reassurance of legal counsel.

For an organization to manage successful website privacy compliance, the CPO cannot work alone; the active involvement of several departments is crucial to the success of privacy compliance efforts. Legal counsel should be closely involved in the privacy team’s activities. The involvement of the internal audit department is also critical, as it can be used to review current and ongoing practices. Similarly, the marketing, web services, customer service and human resources departments, which most often solicit and manage personally identifiable information, are instrumental in the communication and management of issues relevant to privacy policies. As management of these various departments develop new business strategies, it should draw on the knowledge of the CPO to incorporate privacy protections around proposed plans.

Include privacy seals

To make it easier for organizations to explain their privacy policies, demonstrate compliance, and build consumer trust and confidence, online privacy seal programs and independent privacy audits have been created. Online privacy seal programs use graphics to indicate to consumers that the site has been certified according to a set of standards defined by a privacy or consumer advocate group. “I think that privacy seals are a critical component of any regulatory process, whether it’s self-regulatory or government mandated,” says Steve Lucas, senior vice president of Industry Government Relations for...
PrivaSeek, an infomediary (trusted third party) in Louisville, Colo. \(^{11}\) Organizations that issue privacy seals include PricewaterhouseCoopers, TRUSTe, and BBBOnLine, a subsidiary of the Council of Better Business Bureaus.

**Automate website privacy management**

Manual methods of managing website privacy are just too time-consuming and inefficient. Even if your business has hundreds of sites, millions of pages, and thousands of content providers across the organization, there is an automated software solution that enables you to cost-effectively and efficiently manage your website privacy.

Watchfire™ WebCPO™ is the leading privacy management software for your website. Co-developed by Watchfire and PricewaterhouseCoopers, it provides automated, ongoing monitoring, analysis, reporting and alerting solutions to proactively manage website privacy issues. Once your organization has established your privacy practices, you can use WebCPO on a proactive basis to help manage the website privacy compliance issues of your enterprise website. Designed for large, multi-user environments, WebCPO automatically monitors and analyzes all Web properties (Internet, intranet, and extranet) so organizations can understand their information collection, use, and potential sharing practices to help avoid potential privacy glitches. WebCPO analyzes your site and forwards the results of this analysis in a central database. Users can query the database to automatically generate comprehensive reports that identify areas where there may be privacy problems. In addition, privacy officials and auditors are automatically notified via most wireless devices, email, and network broadcast alerts when changes are made to high-risk areas of your website (such as any unauthorized altering of your privacy statement).

The real power of WebCPO lies in its comprehensive reports:

- **CPO Summary Report**: This report provides a snapshot of your organization’s website privacy management challenges by highlighting potential problem areas of your site. Historical reports track changes in your website’s privacy management. The best way to manage your company’s reputation is to know your data collection policies and practices. Understanding your practices will assist you in the development and implementation of sound privacy and security policies.

- **Website Architecture Report**: This report provides information on the size and scope of your website - identifying internal and external links that may pose a privacy risk. Oftentimes, the non-technical website stakeholders in an organization don’t have an accurate picture of the size and scope of their website. This report gives them a snapshot of all their web properties so they can see where internal and external links may be causing privacy problems.

- **Website Data Collection Report**: This report assesses your organization’s practices when information is collected from users with their consent; that is, when they submit data through forms. This allows you to analyze your website’s data collection practices and identify forms that could potentially lead to privacy concerns. This report is critical to understanding the type of notice given to users when they provide information about themselves.

\(^{11}\) “Online Privacy Seals – the Closest Thing to a Guarantee”, by Andrea B. Terry, Bankrate.com, April 26, 1999.
Data Collection Security Report: This report displays the security level of all web pages that contain data collection forms. Information cannot be considered private if it is not secure; therefore, it is important to track the level of security on pages that collect information from users. It is the policy of many organizations to provide a certain level of security for all forms to protect the information entered by users. This report alerts you to instances when forms are not provided with certain security protections.

Privacy Statement Links Report: This report lists all web pages with or without links to a defined privacy statement so you can analyze disclosure practices. Many organizations have a policy requiring that all web pages contain a link to a privacy statement. This report is useful if your organization institutes such a policy and will help you identify where your site does and does not contain links to your privacy statement.

Cookie Report: This report lists all web pages that pass information via cookies (3rd or 1st party) to a web server. Privacy concerns arise when cookies are used for long-term data collection. At issue is whether the company’s use of “cookies” — digital identifiers placed by a web server that track user’s surfing habits - is an invasion of privacy. Generally accepted industry standards recommend that companies disclose their practice of online profiling by third-party ad servers in their privacy statements and provide users with the ability to opt out of receiving cookies. Online consumers may be more willing to interact with your website if they are first made aware of their rights.

Web Beacon Report: This report lists pages using web beacons as tracking devices to gather information about visitors - helping you ensure proper disclosure of web beacon usage to your site visitors. Since web beacons or bugs (clear GIFs or pixel tags) are typically 1x1 pixel in size, they are often invisible to users. There is potential risk exposure for a website if unauthorized tracking devices are present, if authorized tracked devices are capturing inappropriate data, or if captured data is being used inappropriately. This report can help you track when new web beacons have been added to your website. It will also allow you to identify old web beacons that should be removed.

Third Party Links Report: This report lists all web pages with links to external domains. It is important to know what external websites your site links to. Your organization may bear reputation and litigation risks if a linked site has questionable privacy practices. Identifying the linked sites can help you monitor these risks.

Privacy Graphic Search Report: This report provides a list of all web pages that contain images, specifically privacy seals. It also validates whether the link to the association responsible for the Privacy Seal is valid. Many websites post a privacy seal from organizations such as BBBOnline, TRUSTe, or WebTrust. If your website includes these seals, you should monitor these seals to ensure they appear where you expect them to be.

Privacy Text Search Report: This report identifies pages containing words or phrases, such as those that target specific groups (i.e. children) and therefore may pose a privacy risk. The content may be located on the web page, a URL, one or more metatags, or within a form control. This information is very useful in tracking privacy-specific content, and identifies what kind of information the website is collecting that in turn may be used to target specific groups. In order to manage your company’s legal exposure, a heightened knowledge of your site’s data practices is required. Determining what type of data your website collects will determine what regulations apply.
Conclusion

The privacy gap can be closed with sound privacy management practices and automated solutions; furthermore, organizations must close the privacy gap to instill trust in customers and partners. If trust is to be built into the e-business process, privacy and confidentiality must be at its core. Those organizations that understand the risks inherent in their privacy management practices, address the exposures, and communicate their policies openly, will earn consumer and user trust, and are more likely to benefit from customer loyalty and enjoy long-term success.

Benefits of good privacy practices

A systematic approach to comprehensive privacy risk management can help organizations achieve the full benefits of online commerce:

- **Realizing cost savings through automated privacy monitoring.** The size and scope of enterprise websites make manually checking for privacy issues a challenge and the task of ongoing privacy compliance a burden. With sites growing and changing on a daily basis, there are too many issues to allow for cost-efficient and effective manual checking of privacy compliance problems. Automated technology monitors your website on demand, or at scheduled intervals, to help you proactively manage website privacy.

- **Reducing risks of non-compliance with regulatory and self-regulatory frameworks.** Governments around the world are increasingly moving to mandate that the private sector prove it is using good practices, and that individual self-regulatory programs work.

- **Gaining a competitive edge in the information economy by building consumer trust.** Consumers have shown a desire to enter cyber-markets if they have assurances that their privacy will be respected. Companies who can give those assurances—and back up their claims with verifiable privacy policies—will engage the greater portion of the market.

- **Increasing good relationships with partners, who can trust in the security of business partner data.** Where there is a clear policy and disclosure on how business data is shared, partners know where they stand.

- **Increasing good public image, as a leader in privacy protection.** When intimations of bad practices or official censure are unleashed to the public, it is extremely difficult, time-consuming, and expensive for the exposed company to regroup.

- **Reducing risk of further regulatory burden.** Companies ignore good self-regulation at their peril—they are asking for strong regulation when they flout official mandates to do it themselves. Governments will act—and precedent has shown they will act quickly—when commercial interests compromise privacy.
Founded in 1996, Watchfire’s Website Management software and services help organizations optimize their ebusiness strategy execution. Our solutions address critical website issues that can affect visitor success, mitigate corporate risk, and also enhance web team effectiveness. Watchfire’s comprehensive automated testing, analysis, and reporting solutions can help detect and manage issues on even the largest and most complex sites. Our sophisticated reports put detailed, actionable information regarding content and interaction defects, searchability, accessibility, design effectiveness, privacy compliance, corporate standards compliance, and brand equity into the hands of the people who need it, when they need it.

PricewaterhouseCoopers (http://www.pwcglobal.com/), the world’s largest professional services organization, helps its clients build value, manage risk and improve their performance. Drawing on the talents of more than 150,000 people in 150 countries, PricewaterhouseCoopers provides a full range of business advisory services to leading global, national and local companies and to public institutions. These services include audit, accounting and tax advice; management, information technology and human resource consulting; financial advisory services including mergers & acquisitions, business recovery, project finance and litigation support; business process outsourcing services; and legal services through a global network of affiliated law firms.

Other privacy links
(Disclaimer: Watchfire Corporation does not endorse the content of any external website listed here. This list is provided for information purposes only.)

Association of Corporate Privacy Officers: www.corporateprivacyofficers.org
Privacy Officers Association: www.privacyassociation.org
U.S. Federal Trade Commission Initiatives: www.ftc.gov/privacy
Electronic Privacy Information Center: www.epic.org
Privacy Leadership Initiative: www.understandingprivacy.org
Privacy Exchange: www.privacyexchange.org
Health Privacy Project: www.healthprivacy.org
Network Advertising Initiative: www.networkadvertising.org
Online Privacy Alliance: www.privacyalliance.org
Privacy International: www.privacyinternational.org
Privacy Partnership: http://www.truste.org/partners
Australian Privacy Commissioner’s Website: http://www.privacy.gov.au/
The Privacy Commissioner of Canada: http://www.privcom.gc.ca/

What’s next?
This is the fourth white paper in the Bad Things series. Look for a new paper every 4-6 weeks; you’ll automatically receive them because you are already registered. Each paper will be supported by an online Web seminar. Where relevant, these seminars will be held in conjunction with our technology partners. You’ll be notified automatically when this information is confirmed so you can mark your
calendars accordingly. We'd love to hear your comments and feedback about this paper and the Bad Things series as it continues to roll out. Please respond to goodwebsites@watchfire.com.