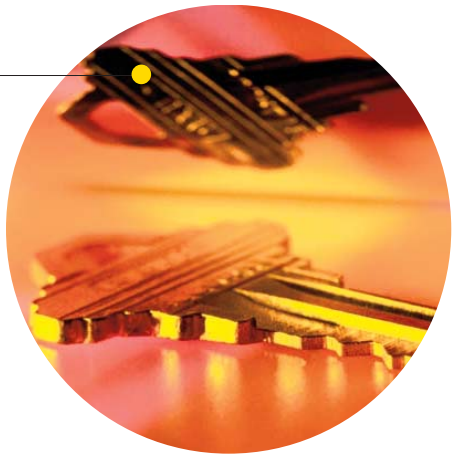
WHITEPAPER

On-Line Privacy Monitoring as Part of an Overall Proactive Privacy Strategy

January 2007



About the Authors:

Kieran Glynn works for the Hewlett-Packard Webgovernace Team in the European Software Centre, Galway, Ireland. Kieran is a Certified International Privacy Professional (CIPP).

Kurt A. Mueffelmann is president and CEO of HiSoftware, a leading provider of software, services, and on-demand solutions that test, repair, monitor and enforce Web content, quality and regulatory compliance.

HiSoftware®

Table of Contents

Introduction to On-Line Privacy Monitoring as a Part of an Overall Proactive Privacy Strategy

The Internet age has revolutionized how organizations communicate, publish and find information. While this technology has created new opportunities for global communication and commerce, it has also created new challenges in risk management.

With the rush to put information "online", many organizations have fallen prey to the exponential growth of Web-based electronic information. The volume of information available through organizational Web sites, Intranets, Extranets and Networks, via multiple entry points, provided by multiple content contributors, in multiple forms and languages, has increased dramatically. Thus, online risk management is a critical component of any successful online business strategy.

What is Online Privacy?

Online privacy is the control consumers have over the collection, use, and distribution of their personal information on the internet. For consumers, the privacy of their personal information is one of the most important technological issues they face today. With the massive rise of the internet and technology in general, protecting consumers' personal data is more important than ever.

Many organizations, both public and private, are mandated by privacy legislation which governs their collection, use, retention and distribution of personal information. These organizations include government agencies, financial institutions, health care organizations and a wide range of other organizations conducting business online. Privacy legislation varies between countries. Private companies may be subject to different rules and standards in different regions of the world, and through different areas of their businesses. Organizations must identify and manage online privacy and risk issues to ensure regulatory compliance, and to earn and retain customer trust.

What are Online Privacy Best Practices?

An online privacy best practices program, provides a model that gives companies confidence in the proper collection, usage and protection of consumer's personal data while also allowing consumers control over their personal data.

Implementing a solution to accomplish this task in the past has been unmanageable and cost-prohibitive to most organizations. Organizations often do not have dedicated IT and personnel resources to allocate to such challenges; however organizations may be at risk for non-compliance without an enterprise-wide solution in place.

An online privacy risk management strategy should give an organization the ability to view policy implementation from a project management perspective, which will enable

the allocation of resources appropriately across an organization and track site progress, as well as identify problem areas so action items can be assigned against them. A good privacy strategy should also provide the ability to integrate testing into any quality assurance and content delivery processes associated with existing Web development and deployment practices. And finally, a user is able to keep a historical view of their testing over time, which is a great way to measure the progress of a project and set goals for the future.

How Do You Know if Your Organization is at Risk?

If your organization has a Web site that collects personal information from consumers, or provides online services to consumers, you are at risk.

Through online technology, consumers now have more personalized and customized services available than ever before. However, with these services the potential for misuse of personal data has increased. As a result consumers have become very concerned with protecting their privacy online. This fear of privacy loss has made many consumers reluctant to provide personal information online, and is hurting e-commerce globally.

The Importance of Creating an Online Privacy Policy

If you want to attract, protect and serve consumers on your Web site, you need to state exactly what methods you use to protect their personal information. This is done through an organization's "privacy policy". A privacy policy assists your visitors in understanding your organizations practices in capturing and/or distributing visitor/customer information that you may require site users to submit. This is particularly important if you require visitors to provide personal information in order for them to access areas of your Web site. If you do not have a clearly documented privacy policy on your Web site, you may risk losing visitors wary of providing their information, and you also may expose yourself to unnecessary risk of litigation.

A privacy policy documents an organization's application of the eight data protection principles to the manner in which it processes data organization-wide:

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to than individual, on request

A Privacy Policy can go into great detail on how an organization applies these principles, what procedures it should follow, assigning individual/departmental responsibilities, etc. A Privacy Policy is fundamentally a document for internal reference.

Alternatively, a Privacy Statement is a public declaration of how the organization applies the data protection principles to data processed on its Web site. It is a more narrowly focused document and by its public nature should be both concise and clear. A Web site privacy statement will outline what type of information is collected on your Web site, how that information is used, how your customers can access that data, and the steps involved to have that data changed or deleted. A Web site privacy statement will also outline how you protect the information of your Web site users. If your Web site uses tracking technology, e.g. cookies, Web beacons, their use must be explained and instructions should be given on how to reject cookie usage.

When designing your privacy statement, bear the following in mind:

1. The most important aspect of a privacy statement is that it must be accurate. i.e. whatever you say you do, make sure you do it. The only thing worse than not having a privacy statement on your Web site, is having an inaccurate one.
2. Use model privacy disclosures and tailor them to your organization's needs. This is not a cut and paste job, but they can be used as a good starting point.
3. Do not use your privacy statement as a disclaimer. Your Web site privacy statement should articulate what is currently happening, not what may or may not happen in the future.
4. Revise your privacy statement periodically as your current privacy practices may change over time or legislation may force these changes.
5. Provide training to all of your employees so that they understand clearly your organization's privacy practices and your Web site privacy statement.

Major Privacy Concerns in the Marketplace Today for Privacy Managers: Why Should Privacy Mangers Care?

Consequences of Privacy Breaches

A privacy breach is a disaster for any privacy manager. The price that organizations pay when a breach becomes public can be catastrophic. On average companies lose 2.1 percent of their market value within 2 days of a breach, which means an average of a $1.65 billion loss in market capitalisation per incident. This does not take into account the losses that result from damaged brand, and reduced customer trust. This is why many firms will do whatever it takes to keep privacy breaches from going public. It should be noted that at a Senate Judiciary Committee in early April 2005, the three largest data brokers in the USA, Choicepoint, LexisNexis, and Acxiom, were asked if any of the companies had a security/privacy breach prior to 1993. All companies

testified that they had. The consumers affected were never informed as notification laws only offered consumers rights after 1993.

Forced to inform consumers by California's disclosure law, ChoicePoint in February 2005 said that it had sold personal data on 145,000 people to criminals posing as customers. ChoicePoint stock lost 1.3 percent the next day, fell nearly 14% the following week was down more than 12 percent from the day of the disclosure. See http://www.bofabusinesscapital.com/resources/capeyes/pdfs/CapEyes_Issue_01_06.pdf

Additionally, ChoicePoint "agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle Federal Trade Commission charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement required ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026." See http://www.ftc.gov/opa/2006/01/choicepoint.htm

In the Jupiter Research report entitled *Online Privacy: Managing Complexity to Realize Marketing Benefits*, Jupiter analysts advised companies to allocate budgets for consumer security and privacy education and to treat online privacy as a strategic marketing differentiator, rather than a compliance exercise. See http://retailindustry.about.com/library/bl/02q2/bl_jmm060302.htm

Based on research and analysis of Consumer Survey data, Jupiter forecasts that as much as $24.5 billion in online sales will be lost by 2006 — up from $5.5 billion in 2001. Online retail sales would be approximately 24 percent higher in 2006 if consumers' fears about privacy and security were effectively addressed.

With poor online privacy practices, many companies will experience negative effects not only on their online sales over the next several years, but also in off-line sales that shift to more privacy-sensitive competitors.

Concerns in the Marketplace Today for Privacy Managers

Privacy managers need to be concerned with a variety of issues that may impact their organizations. These include:

1. **Regulatory Compliance** – Failing to comply with regulatory requirements may result in massive negative media attention, large fines and penalties. Privacy managers must have expert knowledge on privacy legislation across all geographical regions.

2. **Image and Branding** – Breaches in privacy can have a negative effect on an organization's image and brand, and hence its perception as a trustworthy company in the marketplace.

3. **Financial Loss** – Significant financial loss may result from privacy breaches, directly (e.g. credit monitoring service to protect against id theft resulting from data leak on your Web site) or indirectly (e.g. reduced customer loyalty).

4. **Stakeholder Loss** – The price that organizations pay when a breach becomes public can be catastrophic. On average companies lose 2.1 percent of their market value within 2 days of a breach, which means an average of a $1.65 billion loss in market capitalisation per incident. http://info.freeman.tulane.edu/huseyin/paper/market.pdf

5. **Business Partners** – Do your vendors, suppliers, service providers adequately protect your customers data? Sharing customer PII with other companies that might expose customer data to significant risks or misuse is not accepted by customers and is a law violation in some countries. Maximum care and caution should be applied before sharing data.

Best Practices Approach to Managing On-Line Privacy

To determine the significance of such risks to your organization, it is important to conduct a privacy risk assessment. The results of this will determine your organizations privacy program.

In most cases, an adequate privacy compliance program would require:

- Obtaining the commitment and support from senior management
- Delegating responsibility to a privacy official
- Taking inventory of current privacy practices
- Developing privacy policies and procedures
- Educating employees on privacy policies and procedures
- Implementing and monitoring the privacy compliance program
- Automatically *and* continuously monitor Web sites for privacy compliance

Organizations must perform regular self-assessment audits to verify that their privacy policy is accurate, comprehensive, prominently displayed, correctly implemented, communicated and accessible.

Organizations should work with third party testing programs that will provide oversight to the organizations privacy program, and should cooperate with the relevant Data

Protection Authorities in the investigation and resolution of any complaints relating to their policies and should respond to the decisions of these authorities as appropriate.

Web sites should be monitored continuously and automatically to ensure regulatory compliance 365 days per year. Many serious privacy breaches have occurred through poor Web site standards. For organizations with large Web sites, this is essential, as Web pages are updated constantly, sometimes by different business units or outsourced Web design agencies that may not have any communication with each other. Many large organizations will have millions of Web pages, making manual compliance impossible. Web sites are a potential privacy weak point that if not controlled properly, can have dire consequences for an organization. Continuous Web monitoring also provides an excellent illustration of due diligence on the part of an organization.

Automated Privacy Monitoring Solutions from HiSoftware

HiSoftware has recognized the challenges facing Privacy and Web compliance managers today. The company provides software, services, and On-demand solutions that test, repair, monitor and enforce Web content, quality, and regulatory compliance. The company's solutions empower content developers, Web site architects, and executives to work collaboratively to create and manage corporate Web standards for accessibility, privacy, security, search engine optimization (SEO), site quality and performance, branding, competitive intelligence, and application transaction testing (AppTest)..

HiSoftware's AccMonitor Suite, is an enterprise solution that provides automated and repeatable back-end server-based monitoring and reporting, ensuring your organization's Web content and applications meet compliance policies effectively and efficiently. In addition to enterprise server solutions, HiSoftware also offers interactive, user-driven desktop solutions which allow developers to test and remediate content in their development and quality assurance environment.

HiSoftware solutions make it easy to incorporate standards-based compliance into Web design and development practices; a much more cost-effective strategy than the alternative of monitoring for compliance "after the fact". By implementing an automated Web compliance solution, organizations will be able to mitigate risk and ensure compliant Web properties and reduce the man hours spent on testing Web content/applications. Additional benefits include:

- Scans and reports that will identify Web Content that expose the organization to the maximum risk for privacy and accessibility violations to help prioritize projects and resources.
- Reports provide exact locations of errors and this will also further reduce the time it takes to implement fixes and changes.
- Business and policy owners can continuously monitor published Web sites, systems and applications to ensure they continue to conform.

With over 4,000 customers worldwide, HiSoftware has the expertise to help you achieve all of your Web content compliance goals with world-class software, project management, training and consultative services.

Appendix 1—Web site Privacy Statistics-Analyst Reports

2005 Benchmark Study of Corporate Privacy Practices (Ponemon Institute, Vontu)

http://www.vontu.com/news/release_detail.asp?id=352

In a survey that polled 68 large companies with over 1,000 employees across all industries,

- Fifty-six percent of respondents believe that safeguarding privacy has a direct positive impact on their company's brand or image in the marketplace.
- Seventy-nine percent of the polled companies have a separate privacy policy dedicated to employee information and 100 percent of the companies have a privacy policy for customer or consumer data, but only 80 percent have a privacy or data protection strategy.
- Budgets are still trying to catch up to an increased focus on privacy. Only 38 percent of the companies polled believe their resources are adequate to manage privacy requirements and only 31 percent have a formalized notification process in the event of a privacy breach.

Data Security Trends 2005 (Vontu)

http://www.vontu.com/uploadedFiles/global/DataSecurityTrends2005.pdf

- 95 percent of data loss incidents were unintentional. Most breaches were the result of careless or untrained employees, or legacy automated processes.
- 59 percent of violations included private customer information. Last year it was 43 percent.
- 41 percent of violations contained intellectual property, insider information, or trade secrets.
- 58 percent of violations may be subject to review by state and federal regulations, including GLBA, HIPAA, CASB1386, OFAC, SOX, Visa CISP and Full Disclosure Regulations.
- 16 percent of breaches occurred via Web mail, such as Yahoo!, MSN/Hotmail, Gmail, etc.
- The average number of customer data records compromised per breach: 28
- The average number of data loss incidents per year per employee: 4

Appendix 2—Web Site Privacy Breach Examples

DoubleClick – $450k – Cookie usage
Online advertiser DoubleClick was one of the first and most meaningful privacy suits to date. Plaintiffs alleged DoubleClick violated its privacy policy by using cookies to identify Internet users, track the Web sites they visited and obtain other private information about them without consent. Plaintiffs sought to stop DoubleClick from collecting personal information without permission and to have all data already collected destroyed. In a settlement approved by the court in May 2002, DoubleClick was required to educate consumers about their privacy rights, provide notice of data collection, obtain consent before using personal data with cookies, place a five-year expiration on cookies, and submit to an audit to ensure compliance. DoubleClick also reached a settlement with 10 states who filed suit against them for violating privacy restrictions due to its use of cookies to profile consumers based on their Web use. They paid $450,000 to cover the investigative costs of the States.

http://www.doubleclick.com/us/about_doubleclick/press_releases/default.asp?p=282

Tower Records Settles FTC Charges
Security Flaw Allegedly Exposed Customers' Personal Information to Other Web Users
MTS, Inc., and Tower Direct, LLC, ("Tower") have agreed to settle Federal Trade Commission charges that a security flaw in the Tower Web site exposed customers' personal information to other Internet users, in violation of Tower's privacy policy representations and federal law. The settlement will bar misrepresentations in the future, require Tower to implement an appropriate security program, and require audits of its Web site security every two years by a qualified third-party security professional for ten years.

http://www.ftc.gov/opa/2004/04/towerrecords.htm

Petco Settles FTC Charges
Security Flaws Allowed Hackers to Access Consumers' Credit Card Information

Petco Animal Supplies, Inc., a national seller of pet food, supplies, and services, has agreed to settle Federal Trade Commission charges that security flaws in its www.petco.com Web site violated privacy promises it made to its customers and violated federal law. The agency alleges that, contrary to Petco's claims, it did not take reasonable or appropriate measures to prevent commonly known attacks by hackers. The flaws allowed a hacker to access consumer records, including credit card numbers. The settlement requires that Petco implement a comprehensive information security program for its Web site.

The settlement prohibits Petco from misrepresenting the extent to which it maintains and protects sensitive consumer information. It also requires Petco to establish and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of personal information collected from or about

consumers. It requires that Petco arrange biennial audits of its security program by an independent third party certifying that Petco's security program is sufficiently effective to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. The settlement also contains record keeping provisions to allow the FTC to monitor compliance.

http://www.ftc.gov/opa/2004/11/petco.htm

Banking Sector Privacy Breaches

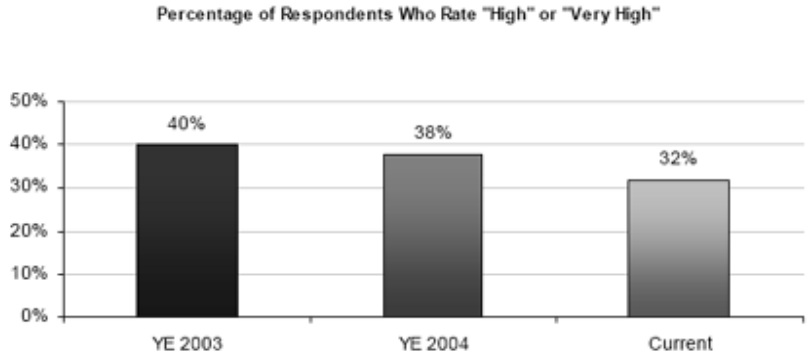
2005 Privacy Trust Survey for Online Banking

Customers with a high degree of trust in their bank are more likely to use online financial services, which generate more profit for banks than offline transactions. The study conducted by the Ponemon Institute, a management-practices research organization, also finds that trusting customers are loyal, with 55% claiming they've never visited another bank's Web site.
The price of that loyalty is an expectation of privacy. Among those with a high level of trust in their bank, 57% indicated that they would stop using online services in the event of a single privacy breach. More than 82% of respondents cited identity theft as their biggest concern should a privacy breach occur.

2006 Privacy Trust Study for Retail Banking (Vontu)

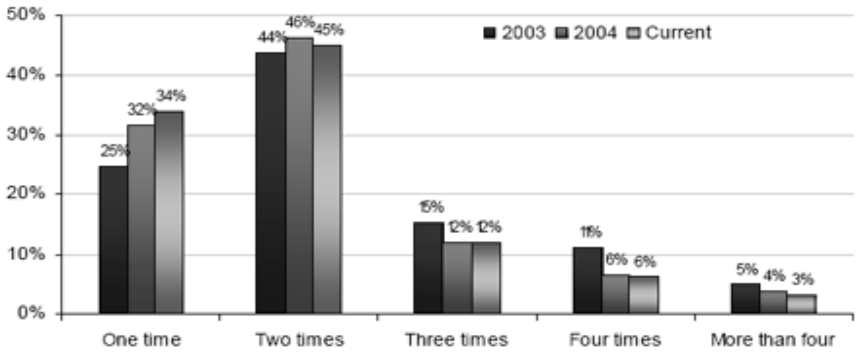
This study reveals that even among banks with the highest level of consumer trust, it only takes two privacy breaches to destroy that relationship. It also shows the customers are less trusting of banks to keep their information secure. In other words, consumers expect their bank to have safeguards and procedures in place to protect them. If consumers lose confidence that their bank is not taking appropriate measures to protect their data from a breach, they will take their business elsewhere.

Bar Chart 3: How Safe is Your Bank in Making Sure Your Personal Information is Secure?



Bar Chart 4 shows a consistent pattern of data collected in all three studies. Respondents do not tolerate more than two or more data breaches.

Bar Chart 4: Number of Data Breaches a Customer will Tolerate



Ponemon Private Research on Data Security Breaches 2004

This study show that the number one cause of a data privacy breach concerns non-malicious employee error. This is usually the result of poor privacy procedures within a company, poor Web site design or insufficient security measures.

Recent Articles on Web site Privacy Breaches

AOL says privacy breach was a mistake (CNN)
http://www.cnn.com/2006/TECH/internet/08/08/aol.search.privacy.ap/index.html

3 Leave AOL Over Security Breach (Washington Post)
http://www.washingtonpost.com/wp-dyn/content/article/2006/08/21/AR2006082100781.html

U.S. Department of Education Web site Exposes Personal Data of Thousands – Aug 2006
http://www.identitytheft911-sunj.com/alerts/alert.ext?sp=615

University of Kentucky tells 1,300 past, current employees that personal data was accessible online – Aug 2006
http://www.kentucky.com/mld/heraldleader/14717374.htm

Virginia Advises Insurance Agents of Security Breach - Aug 2006
http://www.insurancejournal.com/news/east/2006/08/08/71296.htm

E-Health Gaffe Exposes Hospital - July 2006
http://www.wired.com/news/technology/0,71453-0.html

Mississippi secretary of state's office Web site contains thousands of documents containing individuals' Social Security numbers. July 2006
http://www.portauthoritytech.com/datasecuritylabs/leakdetail.aspx?id=71

Personal data exposed on Navy Web site - July 2006
http://www.fcw.com/article95202

Storage Company's Online Security Breach Exposed - June 2006
http://cbs5.com/topstories/local_story_178210503.html

U.S. Government Accountability Office personal data breach - June 2006
http://www.homelandstupidity.us/2006/06/27/gao-discloses-personal-data-breach/

THE AMERICAS

Corporate Headquarters
9 Trafalgar Square
Nashua, NH 03063
Tel 888.272.2484 *(U.S. & Canada)*
+1.603.578.1870
Fax +1.603.578.1876
Email info@hisoftware.com

1711 N. Street NW, 1st Floor
Washington, DC 20036 USA
Tel 888.272.2484 *(U.S. & Canada)*
Email info@hisoftware.com

EMEA
44 Rue Lourmel
Paris, France, 75015
Tel +33 (0) 6 72 51 95 21
Email info@hisoftware.com

www.hisoftware.com