PRACTICAL PRIVACY

Responding to the Rising Cost of Privacy Incidents

A White Paper

By Vincent Schiavone
President& CEO, ePrivacy Group

& Stephen Cobb, CISSP
Senior VP, ePrivacy Group

ePrivacy Group
A trust technology and services company.
www.ePrivacyGroup.com

Practical Privacy:

Responding to the Rising Cost of Privacy Incidents

Abstract: This white paper addresses the unique business challenge of privacy incidents, the risks and costs of which are increasing rapidly. The focus is on practical advice: Prevent and Prepare.

State Attorneys General Weigh In: Privacy Incident Costs Will Escalate

Companies trying to understand the bottom line implications of the privacy issue need look no further than the state of New York. In August alone, New York Attorney General Eliot Spitzer announced three privacy-related actions, two of which imposed six figure fines on well-known, high-tech companies. In effect, Spitzer was making a point: companies that make privacy mistakes, however inadvertent, will face action. Today companies often face simultaneous actions on at least four fronts:

- State attorneys general,
- The Federal Trade Commission,
- Agencies enforcing compliance with privacy-specific laws,
- Individuals.

Announcing that ten states had settled an investigation of how DoubleClick, the Internet advertising service, handled personally identifiable information, Spitzer made it clear that state attorneys general are prepared to enforce consistency of privacy promises and privacy practices:

State attorneys general are prepared to enforce consistency of privacy promises and privacy practices.

> "It's hard for consumers to trust e-commerce when they can't see the practices behind the promises. Consumers need reliable privacy verification—either first-hand, or through an independent and publicized review."

The statement mirrors the FTC's position, expressed by Chairman Muris earlier this month when he announced a consent agreement with Microsoft arising from privacy and security promises about Passport that were allegedly false:

> "Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law."

In addition to paying a fine of $450,000 to New York and the nine other states that joined in the action, Doubleclick agreed to be bound by a consent order that significantly alters the way the company handles personally identifiable information (PII). Just two days later, Spitzer announced another six-figure, multi-state privacy settlement, this time with Ziff-Davis Media, which had inadvertently exposed subscriber PII, leading to several cases of identity theft.

A clear pattern of privacy risk on four fronts emerges.

When you look at this growing list of high profile cases—which includes Microsoft, Eli Lilly, US Bancorp, and Eckerd—there emerges a clear pattern of privacy risk on four fronts. Businesses that are perceived to have broken privacy promises, even by mistake, will draw the attention of privacy-aware consumers, the federal government, the states and, if your business is governed by privacy-specific laws—such as COPPA, HIPAA, or G-L-B—the regulators of those laws, who have the authority to impose fines.

Privacy-aware consumers will seek civil action against companies that make privacy mistakes, either individually or as a class. Simultaneously, privacy advocates will call for investigations by the FTC. The state attorneys general, for whom pro-consumer privacy actions have no political downside and tremendous political upside, will also investigate. The costs add up even before considering any fines for rule violations, such as violating the existing G-L-B Privacy Rule and the impending HIPAA Privacy Rule. Doubleclick paid nearly half a million dollars to settle with the states, on top of nearly $2 million to settle consumer class action lawsuits. Eli Lilly paid $160,000 to states and is bound by a costly twenty-year FTC consent order (with fines up to $11,000 per violation). Microsoft is bound by a similar order, with state action possibly pending.

The fines and consent costs may eventually pale in comparison to the brand damage such cases can cause.

Often the most costly privacy law to violate is the law of the press and public opinion. The fines and consent costs of regulatory and legal actions may eventually pale in comparison to the lingering brand damage and loss of consumer confidence resulting from such cases. When an Eli Lilly regional sales office in Florida violated company privacy policy this summer, the ensuing civil lawsuit filed by a single individual drew national news coverage because the incident was “yet another privacy problem for drug giant.”

According to Forrester Research, a large company dealing with a high profile incident can expect to incur upwards of a million dollars in unbudgeted time and expenses (March, 2001 report). Even for a small dot com such an incident can cost a potentially crippling $50,000. These numbers don't include brand damage or long term costs of compliance with state and federal consent agreements.

Practical Privacy

There can be no doubt that the cost of not immediately identifying and fixing privacy issues will continue to increase. The best advice is clearly to prevent and prepare. Companies should use their limited privacy budgets wisely. At ePrivacy Group we believe in practical privacy and the practical reality is this:

> you must first fix the privacy exposure that creates the highest and most immediate risk to your organization.

After that, the staff you task with privacy should identify and address lesser issues. At the same time, your privacy staff should be educating everyone, from management to line employees, the meaning of privacy in a company context. Plans and procedures must then be created to ensure effective response to, and mitigation of damage from, whatever privacy incidents occur in spite of your good faith prevention efforts. The message is: Prevent what you can. Prepare for what you can't.

The key to prevention is targeting and treating the highest risks, then training the right people.

Prevention: Target-Treat-Train

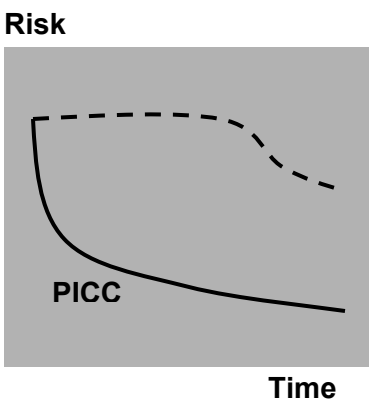
Many companies are straining their privacy budgets and spending too much of their time on massive assessments that leave little room for building and training the sort of team you need to take immediate corrective action after the assessment is complete. A full privacy assessment is seldom the best course of action if your goal is to prevent costly privacy incidents at your company. Indeed, the full assessment approach may increase risk to the organization by identifying problems then leaving them in place.

The Privacy Incident Cost Containment (PICC) risk model identifies and addresses the highest risk privacy issues first.

The more sensible approach is to first target and treat the areas of greatest risk. ePrivacy Group advocates a Privacy Incident Cost Containment (PICC) risk model that looks at a representative sample in key areas of the business to quickly identify the highest risk privacy issues. Through this "triage" process, PICC assures that resources are immediately deployed against the highest risks (a full assessment is more useful after employees are trained and prepared to act).

After you target and treat the biggest risks you will know who needs training and who needs training most. Indeed, training then becomes the key to ongoing privacy incident prevention. If a privacy incident does occur you will find there are no good answers to questions like: "Why didn't you know?" or "Why didn't you prevent this 'obvious' problem?"

ePrivacy Group's PICC model starts reducing privacy risks right away.



Older "assess-then-amend" models prolong risk of privacy incidents.

Without proper privacy training, current privacy exposures can continue undetected and uncorrected, while new ones are being created, just because employees don't know any better. For example, how confident are you that your company has the right answers to the following questions?

- Is IT developing and testing applications using live PII because they don't know any better and there are no policies or procedures to prevent it?
- Is marketing piloting an aggressive new marketing program tomorrow that accidentally violates the privacy of consumers?
- Is legal including privacy in its contract reviews?
- Does legal realize that privacy is now critical in all mergers and acquisitions, as well as many partnerships and joint ventures? The legal department may be aware that just about any contract with a health-related entity now needs to include HIPAA-compliant medical privacy language, but is it aware that the recent Doubleclick settlement requires all companies that use Doubleclick's services to comply with certain privacy standards?

Until employees in all these areas understand privacy and know how to identify potential risks there will be many more new exposures.

Prepare to Recognize, React, Respond

The best way to minimize the cost of internal and business associate incidents, and prevent them from taking on crisis proportions is summed up in the phrase: recognize, react, respond (coined by Michael Miora, CISSP, an ePrivacy Group Senior VP and managing director the company's consulting services).

All too often an organization is notified of a privacy incident by its consumers, the press or regulatory authority. In many cases there is documentation that the employees of an organization had clear indication of a privacy incident and either failed to recognize it or failed to react to it. The only questions worse than, "What did you know?" and "When did you know?" are "Why didn't you act after your knew?" and "For how long after you knew did you fail to act?"

Bad answers to these questions are often directly related to the scope of the ensuing investigation and the cost of the incident. Appropriate employees must have the training to recognize privacy incidents

before the outside world. They need both the means and incentives to react quickly. An interdisciplinary Privacy Incident Response Team—including technical, legal and public relations—must be built and trained to respond quickly and effectively to contain the incident and minimize the risk it poses to the organization. In an environment of multi-million dollar incidents being unprepared is a costly mistake.

Training is the Key

Why is privacy training the key ingredient in both prevention and response? Because it works! Twenty years of experience in security and privacy risk management tells us that training is the single most effective tool to reduce risks.

Many companies react to new laws and regulations by searching for the latest technical solutions and writing the most appropriate legal notices and disclaimers. The practical privacy reality is this: there are no magic bullets. Technology is only part of the solution and technology is only as good as the training of the people who deploy and operate it.

Notices and disclaimers are necessary but they are seldom understood by the consumer and typically ignored by the press as well. If an inadvertent mistake occurs, notices and disclaimers are not effective unless the organization is willing to go to all the way in court. Even if you win in court, you still could lose in the court of public opinion. You seldom read that "Bad Thing Happens to Innocent Consumer: Court Rules She Deserved It—Huge Organization had properly disclosed that anything this could happen and is therefore not responsible."

The better your employees understand privacy, the better they are trained to react to incidents, the better off the organization will be.

A better understanding of privacy across the entire company is a tremendous defense mechanism. The better your employees understand privacy, the better they are trained to prevent incidents, the better they react to any incidents that do occur, the better off the organization will be. In privacy, as in all of business, an organization is only as good as its people, and people are only as good as management encourages, trains, and empowers them to be. As the costs of privacy incidents increase, so does the return on investment for any company that makes an investment in privacy today.

ePrivacy Group's Role

ePrivacy Group is a trust technology and services company. Trust is an essential element of all commerce, especially electronic commerce. Companies that falter as they strive to deliver on privacy promises are being judged unworthy of consumer trust, by the courts of law, press, and consumer opinion. Privacy professionals know that privacy is a large risk that cuts across most departments in a corporation and requires an interdisciplinary team of knowledgeable legal, technical, marketing and PR professionals to identify the risks and protect the corporation.

ePrivacy Group can help you build, train, and staff that team. Our trainers are industry leading experts who provide on-site and on-line training under the aegis of an independent trusted authority. Above all, we believe Practical Privacy is a realistic approach to keeping privacy promises, preventing the preventable, preparing for the inevitable, and thereby minimizing risks and costs to the organization.

Notes:

1. The U.S. Bancorp settlement was with the Minnesota Attorney General for $2,500,000 and arose from sharing of customer account information with third parties for purposes of marketing non-financial products and services.

2. The Eckerd settlement was with the Florida Attorney General for $1,000,000 and arose from failure to adequately disclose the purpose of "prescription receipt forms" at pharmacies, which actually doubled as permission to market to drug recipients.

3. The Toysmart settlement was with the FTC over COPPA violations and required destruction of some data collected, plus limits on the sale of data as an asset in bankruptcy proceedings.

4. The "third" privacy-related announcement from Spitzer's office in August was the indictment of identity thieves who had victimized thousands of New Yorkers by obtaining their PII from entities that included American Express, Hollywood Video, Worldcom Wireless, the New York State Insurance Fund, the Social Security Administration, Empire State College, and WNYC radio. The stolen PII was used to obtain hundreds of thousands of dollars worth of property. The increasing frequency of such crimes is a major factor fueling consumer privacy concerns.

About ePrivacy Group

ePrivacy Group is a trust technology and services company founded by experts in privacy, security, and marketing, known for their consulting and training services to global 2000 companies, government agencies and professional trade associations. Services currently offered include:

- Privacy Officer training,
- Employee privacy training, in person and over the net,
- Privacy strategy, implementation and oversight consulting,
- Privacy incident response management, and
- Technology investigation, strategy, and expertise for regulatory and legal actions.

Using a Privacy Incident Cost Containment (PICC) risk model, ePrivacy Group takes a Target-Treat-Train approach that reduces privacy risks as quickly and cost-effectively as possible, thus enabling companies to keep privacy promises and enjoy the benefits of privacy-positive positioning.

ePrivacy Group's patent-pending Postiva™ technology provides a language and framework of trust, privacy, security and intelligence for messaging.

Postiva technology enables the Postiva Trusted Sender program to assure trust and confidence in email. Postiva Trusted Sender is an industry self regulation program that uniquely combines email best practice principles and advanced technology with certification, dispute resolution and ongoing oversight provided by TRUSTe, the leading non-profit trust authority on the internet,

Postiva Trusted Sender is a cryptographically secure way for consumers, ISPs, spam filters, and email clients to verify the authenticity and integrity of email. Trusted Sender eliminates the threat of bogus or spoofed email for leading brands and consumers by enabling secure, platform independent, email authentication.

Using Postiva technology, ePrivacy Group can provide governments and other entities with email authenticity and integrity verification, delivered as a turn-key solution.

ePrivacy Group is a privately held company with offices in Philadelphia, Washington, D.C., Los Angeles, and Europe. The company web site is at eprivacygroup.com.