Privacy Officers ADVISOR

iapp international association of privacy professionals

The official newsletter of the International Association of Privacy Professionals

July 2004 Editor: Kirk J. Nahra Volume 4, Number 10

Privacy by 3PT: A Management Model

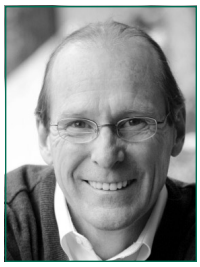
Richard Purcell

Privacy by 3PT is a comprehensive management tool promoting privacy in a purposeful way. The model includes three major communities, four high-level dimensions, and five supporting implementation methods. Over the last several years we have seen the emergence of good privacy practices being actively engaged by organizations for specific objectives and outcomes.

Current pressures from markets, governments, and advocacy groups for privacy controls require active, positive responses from responsible organizations. Privacy by 3PT provides a realistic, sustainable model for these organizations to develop, implement, monitor, and measure data protection and consumer privacy programs that yield long-term value in risk management and customer trust.

Discourse and Discord

Over the course of the last decade, data protection and consumer privacy have been the subject of both discourse and discord, both within and between the United States and Europe. We have established some points of agreement and have agreed to disagree



(for now) on others. These disagreements have tended to be begrudging rather than forgiving. Each side seems to believe that, given time, the other side will eventually see the error of its ways. In other words, we continue to fail to communicate with one another. We can't seem to address the essentials of our positions; we can't understand why the other side "just doesn't get it."

*See **Privacy by 3PT**, page 3*

Britain Narrows its Privacy Law Implementing EU Directive

Amy E. Worlton

Authorities in the United Kingdom recently narrowed the definition of "personal data" under the U.K. Data Protection Act of 1998 and thereby apparently limited the jurisdictional scope of the act that implements the EU Data Protection Directive in the United Kingdom. The act imposes detailed privacy requirements on nearly all businesses operating in the United Kingdom that handle "personal data."

Such businesses must provide notice to individuals as to how their personal data will be used, obtain consent from such persons in many cases, and allow individuals access to their personal data. In Part I, the act defines *personal data* as "data which relate to a living individual who can be identified" from the data themselves or in conjunction with other information in the possession of the business. If data are excluded from this definition, privacy obligations under the act are eliminated with respect to those data.

The *Durant* Case

In December 2003, the English Court of Appeals (Civil Division)

held in *Michael John Durant v. Financial Services Authority* (EWCA CIV 1746) that personal data generally are limited to "information that names or directly refers" to a data subject. In contrast, a "[m]ere mention of the data

*See **Britain**, page 6*

This month:

Privacy Officers Advisor

Editor
Kirk J. Nahra
Wiley Rein & Fielding, LLP
Phone: (202) 719-7335
E-mail: knahra@wrf.com

Section Editors
Kirk Nahra, HIPAA & Medical Privacy
knahra@wrf.com

Philip Gordon, HR & Workplace
pgordon@littler.com

Jim O'Sullivan, Employment
josullivan@spencerstuart.com

Shai Samet, COPPA
shai@pricequotes.com

To join the IAPP, call:
(800) 266-6501

For customer service, call:
(800) 266-6501

Advertising and sales
Phone: (800) 266-6501

Managing Editor
Mike Spinney
Phone: (978) 660-4053
Fax: (207) 351-1501
E-mail: spinzo@earthlink.net

Production Editor
Douglas M. Burnette

Privacy Officers Advisor (ISSN: **1532-1509**) is published monthly by the International Association of Privacy Professionals and distributed only to IAPP members.

International Association of Privacy Professionals
266 York Street
York, ME 03909

Phone: (800) 266-6501

Postmaster:
Send address changes to:
IAPP
266 York Street
York, ME 03909

Subscription price: The *Privacy Officers Advisor* is a benefit of membership to the IAPP. Nonmember subscriptions are available at $199 per year.

Business and circulation:
IAPP
266 York Street
York, ME 03909

Requests to reprint:
Mike Spinney
Phone: (978) 660-4053
Fax: (207) 351-1501
E-mail: spinzo@earthlink.net

Notes from the Executive Director

Who do you know that is leading the fight for effective privacy within an organization? Who is positioned ahead of the curve on emerging issues and building advocacy that translates to a strong top-down approach to maintaining privacy? Who is turning the need for privacy into an essential element to a winning business strategy?

The IAPP is accepting nominations for the 2004 Privacy Innovation Awards, sponsored by HP. There are two awards, commercial and nonprofit/governmental, given to the organizations that demonstrate the most creative approach to meeting privacy challenges.

Each year, as privacy becomes a more complex environment, the level of innovation required to remain on top of the myriad privacy issues that face our community increases.

In 2004, for example, we must consider technical obstacles like camera phones, global positioning systems, and radio frequency identification chips. There are legal issues like the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act (to name just two), and, of course, the self-imposed regulations found in the privacy policies we create and post to help protect and inform our customers.

The price we pay as organizations for ignoring these issues is collected in many ways. State attorneys general and the Federal Trade Commission will be there to tell us when we've slipped up with regard to the law, and public opinion — evident in a lack of consumer dollars — will let us know when we're not maintaining trust.

There to keep the balance is the CPO. Recent action taken against Gateway Learning illustrates, yet again, that privacy is serious business, and even though the fine Gateway Learning agreed to pay was insignificant, that company — whose bread-and-butter is selling a product designed to help children — will certainly feel the cost of public backlash.

Contrast that event with a recent survey that shows adherence to a strong privacy policy directly and positively affects a company's bottom line, and, clearly, the role of the privacy professional has graduated to bona fide mission-critical status.

We want to know so that we can acknowledge their contribution to our community and honor them with some special hardware that will undoubtedly occupy a special place on the mantle.

Check out the "IAPP Announces Call for Nominations for 2004 HP Privacy Innovation Awards" box on page 14 for more information on how to submit your nominations. We'll announce the winner at the Privacy Academy in October.

We look forward to hearing from you.

J. Trevor Hughes
Executive Director

Privacy by 3PT

from page 1

We believe there is more to this lack of alignment than just stubbornness and historical context. One very basic disagreement concerns accountability for the rules of fair play. Both inside and between our regions, we haven't been able to achieve a common foundation for privacy. Yes, many Americans are reluctant to encourage broad government oversight, and certainly many Europeans can't see global corporations as compassionate guardians of public interests. But these dogmatic views are overly simplistic, unhelpful, and do little to help us understand one another.

There is much more at play here than these rigid positions expose. There is a real failure underlying the disagreement, and poking each other with barbs grown dull from decades of use is an unlikely way to tease out a solution. This article does not attempt to produce the solution; we simply recommend a starting place using a management model designed to help us all succeed. If this model provides a newer, sharper stick with which to poke one another, then perhaps it will have served its purpose in seeking a global basis for privacy programs.

We contend that the lack of common agreement in data protection and privacy is quite understandable — it is due to the lack of widely recognized management models specific to this area. Over the last decade, according to experts like Gary Stoneburner, writing for the National Institute of Standards and Technology, concerns about technology security have stimulated the production of security models that have subsequently been implemented in major corporate infrastructures. For the most part, these models have put to rest the disputes over technology security practices; indeed, they have proven to be the catalyst for moving from concept to action.

As a result, we have stopped arguing over the need for security and begun implementing the practices needed to produce a more secure technical environment. Although we have not yet achieved that goal, we are at least on a common path toward it.

Important Opportunity

In the same way, we recognize that we have an important opportunity for developing a professional practice for privacy. Organizations have accepted the value, laws have set expectations and requirements (more comprehensively in some regions than in others), and business leaders generally accept the need for privacy programs in their organizations. We are no longer debating whether we should implement privacy programs; we are only asking "How is it done?"

*See **Privacy by 3PT**, page 4*

3PT

Life Cycles

- **Vocabulary** — defining resources, data, roles, concepts, formats, and rules.
- **Policies** — describing organizational values, principles, infrastructure, legal requirements, and information management.
- **Communications** — for expressing policies and roles, creating awareness, and assessing effectiveness.
- **Data** — moving data through, and out of, organizations.
- **Activities** — guiding information-driven processes such as research, marketing, sales, analysis, worker performance, operations, finance, and administration.

iapp
international association of privacy professionals

International Association of Privacy Professionals

266 York Street
York, ME 03909
Phone: (800) 266-6501 or (207) 351-1500
Fax: (207) 351-1501
E-mail: information@privacyassociation.org

Privacy Officers Advisor is the official monthly newsletter of the International Association of Privacy Professionals. All active association members automatically receive a subscription to *Privacy Officers Advisor* as a membership benefit. For details about joining IAPP, please use the above contact information.

Privacy by 3PT

from page 3

We believe that our management model, Privacy by 3PT, is useful in answering this question. This model is named for its four major components — *people, policies, procedures, and technologies*. These components create a comprehensive model for the design, development, implementation, monitoring, and assessment of privacy programs. This privacy model specifically differs from security models in that it emphasizes behavioral requirements supported by technology. Conversely, security models generally emphasize technical requirements supported by behavior.

Our 3PT model initially examines the roles people play because it is primarily a privacy model more than it is a data protection model, and the latter is largely served by available security models. Privacy, on the other hand, has few if any management models sufficient to cover all the complex needs presented by responsible management of personal information in complex environments. To our knowledge, none deals directly with personal behaviors.

A robust privacy program has to account for the interactions between different kinds of data subjects and types of data controllers who in turn may employ various classes of data processors.

Starting with People

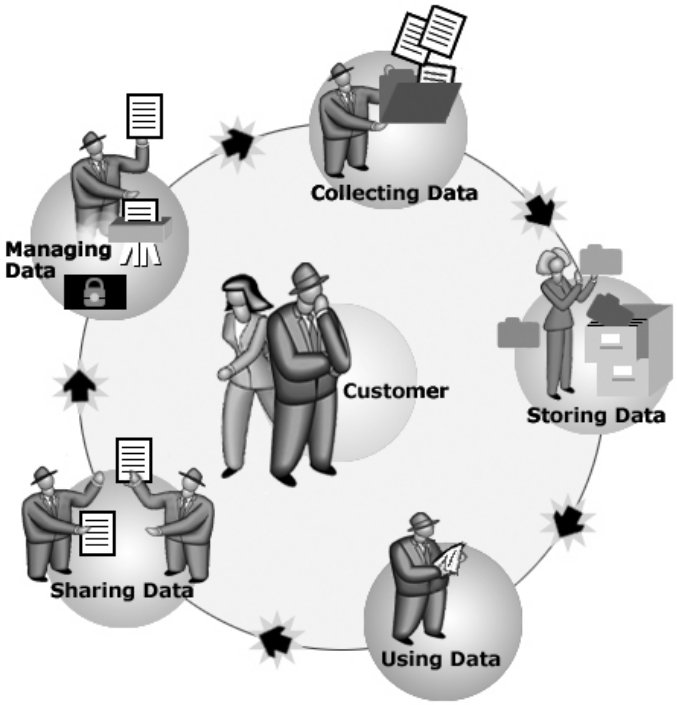
We start, therefore, with people. As in any policy space, there are multiple dimensions to each facet of the issue, and so it is with people. A robust privacy program has to account for the interactions between different kinds of data subjects and types of data controllers who in turn may employ various classes of data processors. For example, a child interacting with a Web site sponsored by a breakfast foods company presents different policy and staffing requirements from those involved when a senior citizen interacts with a retailer selling pharmaceuticals. In each case the data definitions, the policy considerations, the communications, and staff training are significantly different. There is no formula whereby a single sweeping set of criteria apply universally.

The facet of the model called People focuses on several critical challenges. It requires that the data subjects, controllers, and processors are accurately described; that the data is appropriately classified; and that the roles in the data controller and processor organizations are described in detail. Often, this facet involves the identification of workers in specific roles and the development of their knowledge and skills. This and all facets of the model are supported by a series of process methodologies we refer to as *life cycles*. The life cycles involve completing specific processes designed to accomplish discrete goals and outcomes. For the People facet, each life cycle has a distinct contribution. We will discuss the life cycles more fully later.

The Policy facet of the model focuses on the many concerns presented by corporate values, commercial requirements, legal regulations, and market demands. This facet is designed to produce overarching positions that are consistent with business strategies, meaningful to constituents, and acceptable to regulators. The Policy facet is directly supported by a process that develops, assembles, and documents these fundamental positions and aspirations. It is also supported by other methods, including the communications life cycle, which focuses on broad awareness and specific training.

In the Procedures facet of 3PT, we concentrate on pragmatic work issues; it is the most task-oriented facet and

3PT Methods Apply to Life Cycle Processes



Each facet of the 3PT model has associated implementation methods and steps — life cycles — that tend to cycle back on themselves in a continually renewing way to serve individual consumers, employees, and business partners.

requires the most work effort to support. For the Procedures facet, we document the way information is brought into, is processed by, and eventually exits an organization. At each step, the information has to exist within a rich environment motivated by clear rules and guidelines to accomplish the desired outcome. The Procedures facet is supported by life cycle processes that define roles, data, practices, formats, and rules. It is also supported by a communications life cycle designed to inform "the right person using the right channel at the right time."

The fourth facet of the 3PT model, Technologies, recognizes that technical developments including electronic point of sale data input, centralized data processing, and the World Wide Web have created digital information that is easily collected, shared, and used. These same technical developments that are widely seen as exacerbating our privacy concerns also provide valuable privacy solutions. Most of the technical support for data protection comes from tools and software used in data security; encryption, authentication, identification, threat analysis, and other security procedures promote and ensure data protection.

The Platform for Privacy Preferences (P3P) is a technical specification aimed at providing machine-readable support for disclosure practices. Advances in structured database rules like IBM's Tivoli are showing real promise in integrating policies at the level of the data itself. Microsoft's promised digital rights management software may be applicable to personal information protection. Software for Web monitoring like that offered by Watchfire detects rules violations in online environments. Technical means for promoting anonymity like those developed by Zero-Knowledge have promoted individual control. These and other technology developments are beginning to emerge as privacy-enabling technologies (PETs) that support data protection objectives. More than any other, this facet of our model brings together security and privacy practices and objectives.

Processes Rather than Destinations

As mentioned, each facet of the 3PT model has associated implementation methods and steps. We refer to these methods as life cycles because they are processes rather than destinations, and they tend to cycle back on themselves in a continually renewing way. Thus, each life cycle method involves a feedback loop aimed at informing regular analysis and updates.

The steps within each life cycle method are applied to each facet of the 3PT model for each of at least three communities — individual consumers, employees, and business partners.

The life cycle methods and steps include these:

- **Vocabulary**. A method for defining system resources, creating a data dictionary, detailed employee roles, security and privacy concepts, interface formats, and information management rule sets.
- **Policies**. A method for describing organizational values and principles, infrastructure needs, legal requirements, and information management disclosures and practices.
- **Communications**. Processes for expressing policies and roles, creating awareness and training programs, matching messages to appropriate roles, delivering messages using multimedia/multimodal methods, and assessing communications effectiveness.
- **Data**. The ways information moves into, through, and out of organizations, including collection, storage, use, sharing, retention, and disposal.
- **Activities**. Procedures to guide the information-driven processes within large organizations such as research, marketing, sales, analysis, worker performance, operations, finance, and infrastructure administration.

The steps within each life cycle method are applied to each facet of the 3PT model for each of at least three communities — individual consumers, employees, and business partners. These communities may be simple or complex. For example, an employee privacy model might include contract workers, workers in affiliate organizations, and workers in unaffiliated vendor organizations in addition to direct employees.

Sustainable Programs Woven into the Fabric of Operations

Privacy by 3PT is particularly useful in large organizations with multiple locations. It is the only management model that can incorporate cultural and legal norms and standards within a consistent framework. It is also the only model that promotes centralized management, local accountability, reliable monitoring, and consistent reporting. Because it allows flexibility within different jurisdictions without changing the overall framework of the model, it promotes adaptation and application in varied circumstances. This flexibility still maintains consistency in applying privacy protections and data security controls both within the organizations and within its marketplaces. Privacy by 3PT provides value to executives, shareholders, business partners, and consumers. The real beneficiaries, though, are the privacy professionals who are accountable for privacy programs in their organizations. This model provides a solid basis for them to build sustainable programs that will ultimately become woven into the fabric of commercial operations. ■

About the author

Richard Purcell is chief executive officer of Corporate Privacy Group, an independent privacy consulting practice dedicated to supporting the development of sustainable privacy programs. Formerly the chief privacy officer at Microsoft, Purcell serves on the boards of TRUSTe and the IAPP. Purcell can be reached at richard@corppriv.com or (360) 379-0762.

Britain

from page 1

subject" in a document held by a business "does not necessarily amount to [the individual's] personal data."

The case arose when a U.K. citizen attempted to use his right to access personal data under the act as a means to compel a U.K. financial regulator to disclose documents concerning an investigation of a U.K. bank, initiated at the individual's request. In affirming a lower court's refusal to compel such disclosure, the appeals court stated that the act does not constitute a back door for discovery and is limited by its purpose to protect the privacy interests of individuals.

The court offered two notions to help distinguish "personal data," which are entitled to the protections of the Data Protection Act, from "mere mentions," which are not. First, covered information is "biographical in a significant sense" and does more than record a person's involvement in an event that "could not be said to [compromise his privacy]." Second, personal data has the data subject as its "focus," rather than some other person or event.

At root, the court's definition of *personal data* is circular — a person has a privacy interest in personal data under the act if the personal information "affects his privacy." Notwithstanding the possible uncertainty introduced by the court's opinion, however, the *Durant* decision may prove an important step toward greater rationalization of EU data protection law. U.S. companies operating in Europe may well be frustrated by the reach of such laws.

Because operational definitions are written broadly, EU member state data protection laws may require burdensome privacy safeguards when privacy interests are minimal or the risk of privacy injuries is small. Indeed, during the European Commission's 2002-2003 review of the directive's implementation, four EU member states — the United Kingdom, Sweden, Finland, and Austria — remarked that data protection laws impose one-size-fits-all requirements despite varying degrees of privacy risk. In the *Durant* decision, the British court appears to cull out the potential mass of references to persons that technically could fall under the act's definition of personal data but that do not raise issues of privacy infringement.

In affirming a lower court's refusal to compel such disclosure, the appeals court stated that the act does not constitute a back door for discovery and is limited by its purpose to protect the privacy interests of individuals.

Information Commission Guidance

The U.K. Information Commission, the country's independent privacy regulator, recently issued guidance interpreting the *Durant* decision available on the Internet at www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=5152. The regulator stated that personal data under the act must be "capable of having an adverse impact on the individual." The Information Commission clarified that the following types of information likely are "personal data":

- information about the medical history of an individual;
- an individual's salary details;
- information concerning an individual's tax liability;
- information comprising an individual's bank statements; and
- information about an individual's spending preferences.

In contrast, the following would not normally be "personal data" and would not be covered by the U.K. Data Protection Act:

- information retrieved from a computer search on an individual's name or unique identifier, unless such search results specifically focus on the individual;
- a mere reference to a person's name, where the name is not associated with any other personal information (*e.g.*, a list of attendees in the minutes of a business meeting); and
- a listing in an e-mail header of a person's e-mail address when the subject of the e-mail does not concern that person. ■

The U.K. Data Protection Act and the *Durant* Decision

Personal data entitled to the protections of the Data Protection Act:

- Data that is biographical in a significant sense
- Data that does more than record a person's involvement in an event
- Data that has the subject as its focus

Mere mentions not covered under the act:

- A record of a person's involvement in an event that could not be said to compromise privacy
- Data with the focus on some other person or event

About the author

Amy Worlton is an associate with the law offices of Wiley Rein & Fielding. Her practice areas include Internet and e-commerce, privacy, and communications, and she advises clients on international and domestic privacy and security issues including the Homeland Security Act, the Patriot Act, the safe harbor, the national Do Not Call Registry and CAN-SPAM. She can be reached at (202) 719-7458 or via e-mail at aworlton@wrf.com.

Private Offices that Aren't

Protecting Conversations that Must Not Be Overheard

Fred Folsom

The facts are clear: typical private offices do not provide confidential speech privacy. In fact, listeners located outside such offices can overhear and understand most conversations that take place within.

This conclusion comes from the results of a yearlong collaborative study of private offices by Dynasound, Armstrong World Industries, and SMED International. The project was coordinated with the aid and support of the International Facility Managers Association and involved 40 major organizations with more than 30 million square feet of business facilities across America.

Most business managers and executives presume that when they go into their offices and close the door, their conversations are secure. This is far from reality. These studies show that typical private offices achieve only a "poor" speech privacy rating or classification. In this low privacy level, conversations can easily be overheard and understood from outside the room.

The results of the situation are alarming and generally encompass two aspects:

1 Sensitive conversations. Conversations about employee personal matters, confidential business plans, product development, and so on are all compromised when listeners located outside these offices are able to overhear *and understand* critical conversations.

Recent "privacy" legislation has placed increased attention on the right to privacy of individual employees, financial customers, patients and health care consumers, and the like. This compounds the problem of sensitive conversations that are easily overheard. In medical offices, patients overhearing the doctor's conversation in an adjacent treatment room is a well-recognized problem. In most doctors' offices and clinics, this has become a patient satisfaction issue that demands attention.

One factual example makes the point. In the recent past, a Fortune 100 corporation was forced to undergo an extensive investigation by the federal Securities and Exchange Commission because an employee, passing by an executive meeting room, overheard the predictions for the next quarter's strong financial performance. That employee called their broker, and the events that followed created a sudden and significant run-up in the stock price before the financial results were announced.

2 The staggering losses of U.S. trade secrets. There is general agreement among security professionals that most corporate executives in America are not adequately informed about the magnitude of the loss of trade secrets and proprietary intellectual property.

Most business managers and executives presume that when they go into their offices and close the door, their conversations are secure. This is far from reality.

Corporate intellectual property in general is not secure and can easily be obtained. Some of the frequent items on the list of "breech points" are IT networks, disloyal employees, e-mail, and critical conversations that are intercepted by either casual or deliberate listeners inside the facility or from electronic eavesdropping by numerous devices.

In November 27, 2002, President Bush created the new Office of the National Counterintelligence Executive. Each year, the executive reports to Congress on the level of industrial espionage in the United States.

The 2002 *Annual report to Congress on Foreign Economic Collection and Industrial Espionage* contained these alarming estimated losses — due to theft (foreign and domestic) — of the value of corporate proprietary information and intellectual property in the United States.

The estimates listed below were prepared by the American Society of Industrial Security, the U.S. Department of Commerce, and PricewaterhouseCoopers:

- Fortune 1000 companies lost more than $45 billion in 1999 from the theft of their proprietary information;
- in 2001, estimates of losses from the same activity increased to $59 billion; and
- in 2002, loss estimates are as high as $300 billion per year and rising.

Key findings in the 2002 report also included this statement:

> The United States was a prime target for foreign economic collection and industrial espionage, and for the theft of export-controlled proprietary information in 2001. Foreign countries and companies used U.S. technologies to leapfrog scientific hurdles that would otherwise have impeded their military and economic development.

Part 1 — Traditional Private Offices

This section highlights the key points and summarizes the effectiveness of the acoustical corrections to private offices, including the addition of sound-masking solutions. Recommendations included in this article will enable new offices under construction, as well as most existing private offices, to be upgraded in a

*See **Offices**, page 8*

Offices

from page 7

cost-effective manner to achieve confidential speech privacy with minimal construction activity.

Why Most Private Offices Lack Confidential Speech Privacy

- The lack of confidential speech privacy in private offices comes from the reality that there are too many sound leaks from typical interior materials and construction practices.
- Traditional interior design selects ceiling systems, walls, and doors that are laboratory tested and rated *individually* for acoustical performance.
- These components are not laboratory tested according to specific field installation and do not factor in job-site construction conditions such as utility penetrations and construction tolerances. The results are sound leaks and reduced speech privacy.
- Most conventional acoustical ceilings are laboratory tested without light fixtures, air diffusers, return air grilles, sprinkler heads, and such. Each of these penetrations, which occur in "as built" installations, cause additional sound leaks that significantly lower the published Ceiling Attenuation Class (CAC) ratings of ceiling sound transmission.

To address this problem, the collaboration's private office acoustical tests (performed at Armstrong's laboratory) included the ceiling penetrations listed above. The results paralleled "as built" performance of private offices. The same is also the case with the SMED Life Space movable floor-to-ceiling wall system and its respective penetrations. There were two "as built," fully equipped offices constructed inside the acoustical test chamber in order to obtain "real-world" performance data on sound transmission effectiveness.

More efficient heating, ventilation, and air conditioning systems; improved electronic ballasts in recessed lighting systems; and a host of other component improvements combine to result in a much lower building background sound level.

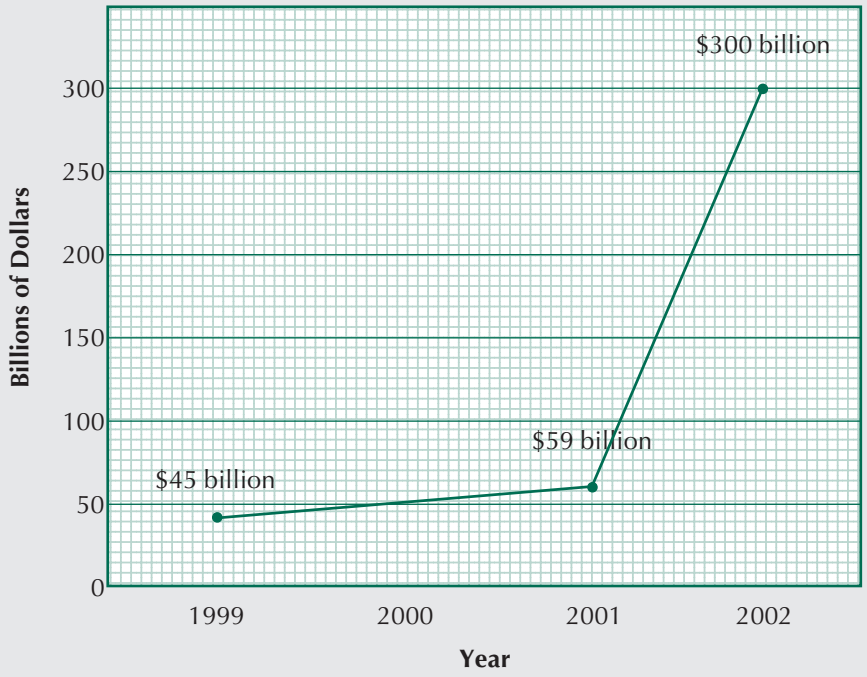
Another important explanation for the lack of speech privacy in most office buildings is that today's offices are significantly quieter than in the past. More efficient heating, ventilation, and air conditioning systems; improved electronic ballasts in recessed lighting systems; and a host of other component improvements combine to result in a much lower building background sound level. Unfortunately the consequence is that sensitive conversations are more often overheard.

The introduction of sound masking corrects the problem by slightly raising a building's sound level. As seen in the test results, the use of a properly designed and installed sound-masking system is a critical element in increasing speech privacy levels. This inhibits individuals located in other areas from overhearing and understanding conversations from inside private offices.

Current Speech Privacy Levels in Typical Private Offices

The collaboration site tests, as well as laboratory analysis of speech privacy performance, showed that the typical private office currently has a privacy level of only 75 percent. (Confidential speech privacy requires 95 percent to 100 percent privacy.) This represents a total loss of all speech confidentiality and presents an unacceptable security risk of corporate intellectual property.

Corporate Economic Losses from Industrial Espionage in the United States



Three Key Components to Achieve Confidential Speech Privacy

- Use ceiling-high fixed or movable partition systems having a minimum 35 STC (sound transmission class). Provide appropriate ceiling and floor gaskets and ensure that doors and door gaskets create a good sound seal.
- Use lay-in suspended ceiling systems that span across the floor plan. Whenever possible upgrade the ceiling system sound absorption performance to .70 noise reduction coefficient (NRC) while maintaining a minimum 35 CAC. The higher sound absorption will help absorb and reduce the speech intelligibility within the room before it infiltrates into adjacent offices. Also, provide a baffle *(*attenuator*)* over the top of all open return air grilles.
- Install a properly designed, installed, and tuned sound-masking system for all private office areas. Masking will slightly raise the building's background sound level and inhibit occupants located outside these offices from being able to hear and understand speech intelligibly.

The collaboration found that because of the various sound leaks that occur with "as built" interior components, it would be virtually impossible to provide confidential speech privacy with partitions either stopping at or passing through the ceiling line without the use of a well-designed, installed, and tuned sound-masking system.

The Collaboration's Test Results

The two private offices constructed inside the acoustical test chamber **achieved a 100 percent speech privacy level at normal voice levels and 95 percent privacy level at raised voice levels.** Both achieve confidential speech privacy as described by ASTM test procedures.

Part 2 — Protecting Mission-Critical Areas Against Inadvertent orElectronic Eavesdropping

Today, far more sophisticated applications of sound masking are available to protect top-secret or proprietary information from either inadvertent or deliberate electronic eavesdropping (*i.e.*, laser beams and parabolic microphones aimed at executive conference room windows). High-security solutions include specialized masking products for many areas in offices.

These very specialized audio security sound-masking solutions have been designed and installed since 1975 to protect against either inadvertent or deliberate electronic eavesdropping of conversations in corporate offices, research centers, government offices, defense contractors, and military facilities. This loss can come either from listeners who happen to be nearby and inadvertently overhear conversations or from deliberate electronic eavesdropping.

A significant concern is to protect against the threat of sensitive conversations being intercepted by the host of electronic devices that are readily available on the open market. One of the more publicized tools is laser beams/parabolic microphone that can be aimed from considerable distances at windows and capture information that can be processed into intelligible conversation.

Leading security experts nationwide indicate that the pace of security investments needs to significantly increase in order to parallel the current level of electronic espionage.

Since 9/11, more and more government officials, as well as a growing cadre of corporations, are taking steps to increase the security of their valuable intellectual property. Yet, leading security experts nationwide indicate that the pace of those security investments needs to significantly increase in order to parallel the current level of electronic espionage.

The information listed below was published in November 2003 by Primedia's *Security Beat Newsletters* and provides an eye-opening call to action on the subject:

- 317 business executives were interviewed;
- 88 percent rate security as a top or high priority;
- two in three companies adopted new security standards in the past 12 months;
- 71 percent rated that their security initiatives will yield positive return on investment;
- 83 percent of companies have conducted risk assessments in the past 12 months — in physical security, IT security, and financial management security;
- only one-third of these company executives felt their security actions are "best practices"; and
- they question if their efforts are the right ones to take.

Extensive experience with eavesdropping protection and sound masking has shown that typically the critical areas of most concern are these:

- board rooms;
- executive conference areas;
- corporate research and development facilities, conference rooms, and pilot plants; and
- executive offices.

For eavesdropping protection to be effective, a variety of specialized sound-masking devices are used that cover a broad range of specialized applications. Among these solutions are masking devices to treat —

- exterior or interior windows;
- walls and doors;
- HVAC ducts;
- utility penetration; and
- ceiling plenums.

Eavesdropping vulnerabilities abound in the typical office environment, and as the risks involved with maintaining individual privacy continue to increase, taking preventive steps to plug audible holes in security should be considered as part of a comprehensive privacy and security strategy. ■

About the author

Fred Folsom is executive vice president of Dynasound Inc., the nation's leading provider of design-build sound-masking solutions to a wide range of corporate and government clients. He can be reached at folsom@dynasound.com or (800) 989-6275 ext. 20.

IAPP in the News

Continuing Coverage from the IAPP/TRUSTe Symposium: Privacy Futures

IBM/Zero Knowledge Lawsuit Gets More Ink

The spat between Zero Knowledge and IBM received additional coverage, as did the IAPP/TRUSTe Symposium: Privacy Futures, in U.K.-based programmer Web site UK.Builder.com.

uk.builder.com/architecture/web/0,39026570,39209663,00.htm

RFID Story Has Legs

Susan Kuchinskas' story on radio frequency identification and the mounting concern over consumer privacy appeared in a number of additional Web sites following initial coverage on enterpriseplanet.com. In the weeks following the conclusion of Privacy Futures, the story also appeared on Wf-FiPlanet.com and InsideID.com.

www.wi-fiplanet.com/news/article.php/3366811
www.insideid.com/trends/article.php/3368641

Other RFID Coverage

Additional exposure for the IAPP was realized when a brief item appeared on the online RFID portal, RFID Gazette.

www.rfidgazette.org/2004/06/rfid_privacy_is.html

Trusted Companies Announced at Privacy Futures

The Ponemon Institute and TRUSTe announced the results of a study to determine consumer trust in corporate brands. The results of the study were released during the Privacy Futures symposium, with resulting coverage appearing in *Darwin* magazine.

www.darwinmag.com/read/060104/ponemon.html

The *Washington Internet Daily* covered events at Privacy Futures in their June 15 issue, including reports from the California legislators' panel and a presentation by the FTC's Dan Caprio.

www.warren-news.com

FTC Big Draw at Privacy Futures

FTC Commissioner Howard Beales' appearance at the IAPP/TRUSTe symposium proved to be a big draw, and he used the opportunity to break important privacy news from the commission. In addition to previously reported coverage from CNET, Beales and the symposium were later mentioned in other online organs, including PrivacyKnowledgeBase.com and IMediaConnection.com.

www.privacyknowledgebase.com/homepage.jsp
www.imediaconnection.com/content/3689.asp

Other Miscellaneous Privacy Futures Coverage

Brian Arbogast's discussion of Microsoft's efforts to beef-up privacy protections was distilled from a story filed for InternetNews.com and included on TechCritic.com.

www.tech-critic.com/print.php?id=9923

In Non-Symposium IAPP News

IAPP Vice President and Nationwide Insurance Companies CPO Kirk Herath was included as a major source in a *Computerworld* article on California's Online Privacy Act. Jaikumar Vijayan, *CW*'s privacy beat reporter, dealt with the issue of collecting personally identifiable information and talked about the effect on online privacy statements with Herath.

www.computerworld.com/securitytopics/security/privacy/story/0,10801,94061,00.html

Privacy News

Dan Caprio Named Commerce Department Chief Privacy Officer

Dan Caprio, former senior advisor to the Federal Trade Commission, was chosen as chief privacy officer for the Department of Commerce.

In a statement issued announcing Caprio's selection, Commerce Secretary Donald L. Evans said, "I am delighted to announce that Dan Caprio will serve as the Commerce Department's new chief privacy officer. In addition to his role as deputy assistant secretary for technology policy, Caprio will oversee all departmental activities related to the development and implementation of federal privacy laws, policies, and practices.

"Mr. Caprio's experience in information security, privacy, and global electronic commerce make him the ideal candidate to carry forward the administration's

commitment to economic prosperity through protecting the privacy of and free flow of information. I am pleased Commerce will continue to play a leadership role for the federal government in this area with Mr. Caprio leading our efforts."

IAPP Board Members Cited in Privacy Article

Board members Kirk Herath, Sandy Hughes, and Barbara Lawler, along with Dr. Larry Ponemon, were cited as primary sources for an excellent article on the value of privacy and the dangers of neglecting corporate responsibility to protect customer information.

Written by Gregory J. Millman, the article appeared in *Financial Executive* magazine and can be viewed online at accounting.smartpros.com/x44287.xml.

COAST Software Unveils Web Compliance Management Platform

COAST Software announced the release of COAST WebCentral, a fourth-generation enterprise solution for managing Web compliance standards that is an automated solution allowing organizations to continually monitor and enforce standards for privacy, accessibility, information assurance, and Web governance.

Commenting on WebCentral's release, Gene Alvarez, vice president, technology research services at META Group, said, "Compliance issues are a hot topic for Fortune 2000 and government organizations today. It is imperative that organizational standards are established and enforced to govern online operations in conjunction with other compliance activities."

COAST WebCentral's advanced server-based technology allows organizations to pinpoint compliance violations in order to build customer trust, secure information assets, and protect revenue streams.

"With COAST WebCentral, we have delivered a best-of-breed solution that has evolved to meet the needs of enterprise customers both from a technology and a business perspective. The comprehensiveness, flexibility, and reliability of this solution make it an easy decision for companies to choose COAST," said COAST CEO and President Paul Saunders.

Law Firm Establishes Privacy Blog

A new blog from the law firm of Hughes & Luce, LLP — PrivacySpot.com — provides readers with original content on current privacy subjects, looking at both sides of issues and providing commentary as to how new developments will affect American businesses. The site also contains links to current privacy-related headlines around the world and a directory of other important privacy sites, including links to data protection authorities and privacy laws in jurisdictions around the globe.

"We wanted to offer companies a one-stop source for information regarding privacy," said Heath Dixon, one of the attorneys who worked to launch the site. "The stories are brief recaps of current privacy events, with links to more information. We will also periodically include in-depth articles focusing on privacy and data protection issues, particularly compliance with laws and regulations."

Stories cover categories such as the FTC, cases and lawsuits, technology, e-mail, legislation, and international issues. Users can register at the site, which allows them to post comments and maintain a personalized list of bookmarks to privacy sites.

Recent topics covered on the site include a challenge to Utah's antispyware law, camera phones in courts, shredding documents, California's e-mail privacy bill, U.S. government scanning of private databases, and *Reason* magazine's cover story on privacy in America.

The blog is the product of Hughes & Luce's new privacy group, which advises clients about compliance with privacy and data protection laws and managing the privacy and data protection risks associated with technology transactions, health law, lending, and employment.

The site can be found at www.privacyspot.com.

COAST Conducts Privacy Compliance Survey

COAST Software recently announced the results of an industry survey, undertaken with Ziff Davis Media and conducted by the Strategy Group, that revealed organizations are exposing themselves to substantial risk from a lack of understanding and enforcement of compliance standards on their Web sites.

Based on a survey sample that included Fortune 2000 representation from industries such as financial services, pharmaceuticals, manufacturing, and government, notable highlights include these:

- almost 40 percent of respondents indicated they don't know which regulations apply to their organization;
- almost 70 percent of respondents foresee serious consequences for failing to comply with standards including lost revenue, lost customers, and negative media attention; and
- more than 50 percent of organizations surveyed are still using manual testing to monitor sites for standards compliance — an ineffective and inefficient practice for sophisticated organizations.

"Effective compliance strategies provide an opportunity to build trusted relationships that strengthen reputation and brand," explains Dr. Larry Ponemon, founder of the Ponemon Institute, who wrote the report's forward. "Given the importance of today's Web sites, organizations must ensure Web properties continually meet the expectations of customers and employees."

To obtain a copy of the report, visit www.coast.com.

knowledge net

KnowledgeNet New York Covers CPP Progam, California Legislation

New York IAPP and TRUSTe members turned out in force for the June KnowledgeNet meeting in midtown Manhattan. The lunchtime event, sponsored by Ernst & Young, featured several lively discussions focused on timely privacy issues. First, there was an open forum regarding the IAPP Certified Privacy Professional Program, where several members offered their comments and suggestions for developing the important CPP program. The group then discussed topics and formats to help shape future KnowledgeNet meetings in the Big Apple.

The general consensus in New York is to offer a variety of formats from formal educational lectures and offering continuing legal education credit to more informal discussions of how privacy professionals address real-world challenges. Case studies from privacy pros involved in critical privacy issues would be enlightening for everyone.

Finally, there was spirited discussion of California's privacy legislation. But the true benefit of the recent KnowledgeNet meeting is that it offered members a chance to network in a fun, informal setting. Look for the September NYC KnowledgeNet to be an even bigger event. We hope to see you there. ■

Submitted by Alan Chapell, president, Chapell & Associates, NYC KnowledgeNet local chair.

Matthew Ellis, senior manager, Deloitte; Laura Becking, partner, Donahue & Partners LLP; Alia Schattauer, data privacy officer, Americas, Deutsche Bank

Alan Chapell, president, Chapell & Associates; and Carolyn Hodge, senior marketing manager, TRUSTe

Shai Samet, chief operating and privacy officer, Referral Technology Inc.; and Lisa Sotto, partner, Hunton & Williams

Save the date for the IAPP/TRUSTe KnowledgeNet lunches coming this fall!

Boston	September 22
Washington, D.C.	September 29
San Francisco Bay Area	October 6
New York City	October 12
Chicago	November 10
Atlanta	November 18
Philadelphia	To be determined

Please check www.privacyassociation.org for updates!

Phishing — The Most Troubling New Scam on the Internet

Michael Weider

What do Bank of America, Visa, Citibank, eBay, PayPal, Wachovia, and Wells Fargo have in common? Besides being some of the best-known names in corporate America, they've also been the victims of *phishing*, a rampant practice on the Web that aims to steal personal information from unsuspecting online customers.

Here's what typically happens in a phishing scam: a spoofed e-mail, complete with legitimate-looking company names, logos, and Web links, that pretends to require verification of personal financial information arrives in your inbox. The embedded link looks authentic, as does the Web page you land on when you click the link. But behind the spoofed Web page, personally identifiable information is being collected and sent to an unauthorized Web server.

A New Type of Phishing

When phishing first appeared over a year ago, the scams were fairly evident, and only the most gullible were vulnerable. According to *Ecommerce Times*, approximately 57 million adults received a phishing e-mail in 2003. Worse, 11 million of those recipients clicked on the links in that e-mail. ("Can the Good Guys Win the Phishing Wars?" *Ecommerce Times* [http://www.ecommercetimes.com/story/33807.html]).

Today, the deceptions are more sophisticated, with the newest kind called "layered sites." Australian bank Westpac was hit with this latest rendition in March 2004. E-mails offered links to a Web site that successfully imitated the bank's site, but the authentic site was "overlayed" so when financial data was extracted, the fake site disappeared and the real site emerged. What's particularly troubling is that customers who don't pay attention to the fade-out might not even realize they've been scammed.

The Cost of Phishing

This new scamming practice will, unfortunately, add to the jittery nerves of online customers and to those who are already hesitant to bank online. This can result in a loss of trust and damage to your organization's brand and reputation, lost productivity while employees help distressed consumers, potential liability to reimburse customer losses, and even legal implications.

According to a recent Gartner Research study, phishing scams cost U.S. banks and credit card companies $1.2 billion in damage last year.

Not only is phishing a huge customer relationship and legal headache, it's a *costly* headache. According to a recent Gartner Research study, phishing scams cost U.S. banks and credit card companies $1.2 billion in damage last year. In the United Kingdom, *The Register* reported that these scams have cost British banks more than £1 million over the last 18 months.

How Your Organization Can Protect its Customers

So, what can you do to protect your customers and your business? You need to create a secure, trusted environment and assure your customers that they can safely continue to do business with you. Here are some suggestions for doing just that:

- Use automated online monitoring solutions that can proactively alert you when company trademarks and brand names are being misused online. Detecting phishing scams as early as possible will give you more lead-time to execute your response plan.
- Scan your Web site with an automated solution for cross-scripting vulnerabilities. This common Web application flaw is used to trick users into thinking they're brows-

*See **Phishing**, page 14*

Tips to Help Your Customers Avoid Taking the Bait

- Use automated online trademark monitoring.
- Scan your Web site for cross-scripting vulnerabilities.
- Deploy strong authentication.
- Scan for similar registered domains.
- Educate customers.
- Develop an action plan.
- Establish notification procedures.
- Proactively warn customers about phishing.

Phishing

from page 13

ing a trusted site when they really aren't.

- Deploy strong Web site authentication, mail server authentication, and digitally signed e-mail protocols with both gateway and desktop verification.
- Scan the DNS to see if similar domains are being registered. For example, when Visa was targeted in December 2003, the phisher used the domain visa-security.com.
- Educate customers so they understand phishing and are familiar with the types of information your organization will and will not ask of them.
- Put an action plan in place to communicate to customers that a phishing scam has been detected and what your organization is doing about it.
- Establish procedures to notify law enforcement of detected fraudulent Web sites.
- Proactively warn customers about the dangers of phishing scams. Banks that can stay ahead of the phishers have a better chance of retaining their customers' goodwill and their online business. ■

About the author

Michael Weider is founder and CTO of Watchfire, a Web site management software and services company based in Waltham, Mass., that helps organizations detect and manage Web quality, Web privacy, and Web accessibility issues on enterprise Web sites. He can be reached at (781) 810-1450 or by e-mail at mweider@watchfire.com.

IAPP Announces Call for Nominations for 2004 HP Privacy Innovation Awards

Second Annual Award for Commercial and Government/Non-Profit Privacy Integration Is Most Prestigious in Industry

The International Association of Privacy Professionals has issued a call for nominations for the 2004 HP Privacy Innovation Awards. Cosponsored by the IAPP and Hewlett Packard, the Privacy Innovation Awards are presented annually to organizations in both commercial and government/not-for-profit sectors that have shown exemplary support for privacy issues and leadership, integrating effective privacy protection throughout the entire organization's business process.

Nominees are judged based on level of innovation, thought leadership, and effective integration of successful privacy programs as part of an overall business strategy.

Studies have shown that investments in effective privacy programs pay dividends through increased revenue and positive public perception. The HP Privacy Innovation Award serves as a catalyst for organizations to examine their approach to privacy and consider ways to implement new and effective privacy programs, allowing them to reap the benefits of greater consumer and citizen satisfaction, enhanced customer relationships, and the competitive advantages driven by privacy-enabled models.

"There is not sufficient recognition for organizations that have embraced privacy as a competitive advantage and a business or governmental imperative," said IAPP Executive Director Trevor Hughes. "The HP Privacy Innovation Award helps to shed light on some of the amazing work being done to integrate privacy as part of an effective business strategy. As such, it has emerged as the most prestigious award in the industry."

"The HP Privacy Innovation Award recognizes the important work that organizations do to enhance data privacy processes," said HP Data Privacy Officer Dan Swartwood. "We want both businesses and organizations around the world to be recognized for their great work in privacy."

Nominations are being accepted from July 1 through October 1. Winners will be announced during the 2004 IAPP Privacy Academy, October 27–29 in New Orleans.

Nominations can be submitted online at www.privacyinnovation.org/nomination/index.php.

Document Retention in the Digital Age: How Long Is Long Enough?

Philip L. Gordon, Esq.

The advent of the "paperless society" has been a boon for fastidious record keepers and the lazy alike. With storage capacity expanding to unfathomable dimensions, and storage costs per bit of data approaching zero, the incentive to discard, at least at first blush, has been virtually eliminated.

However, another trend, the rapid increase in the number of lawsuits, as well as the ever-present risk of government enforcement actions, provide ample justification for doing more than letting data float in cyberspace wholly unattended.

Retrieving data in response to a request for "electronic discovery" in private litigation or in response to a government investigative demand, and the attendant review of that data by attorneys for responsiveness, privileged communications, and confidential business information, could be extremely costly. At the same time, any business person who recalls the 18-minute gap in the Watergate tapes or the rapid demise of Arthur Anderson will recognize that the inability to produce key documents when called upon to do so can be damning not only in the courtroom but in the arena of public opinion as well.

Any business person who recalls the 18-minute gap in the Watergate tapes or the rapid demise of Arthur Anderson will recognize that the inability to produce key documents when called upon to do so can be damning not only in the courtroom but in the arena of public opinion as well.

Recent Federal Court Decision Sheds Light on Data Retention Requirements

A recent employment discrimination case in the federal district court in Manhattan, *Zubulake v. UBS Warburg, LLC,* illustrates the potentially high cost of electronic discovery and provides important guidance for those trying to determine just how much and which data should be retained. In that case a securities trader, Laua Zubulake, charged UBS Warburg, her employer, with gender discrimination and retaliation.

Zubulake requested, in discovery, the production of all communications, including e-mail, relating to her that were sent or received by five specified employees over a two-and-one-half-year period. UBS estimated the cost of restoring and searching backup tapes potentially containing responsive e-mail at $166,000 and the cost for attorney and paralegal review of all retrieved e-mail at $107,000. In other words, responding to just one discovery request would cost UBS more than one-quarter of a million dollars.

To complicate matters further, UBS determined that seven backup tapes potentially containing e-mail responsive to this one discovery request had been destroyed, setting the groundwork for Zubulake's request that the court sanction UBS for destroying evidence.

In three separate opinions, issued between May and October 2003, the court laid out several principles that should guide the drafting and implementation of an effective data retention policy:

- electronic documents are subject to civil discovery in the same manner as paper documents;
- the responding party must bear the entire cost of producing electronic documents in accessible format, in other words, stored in a readily usable format;
- the court will shift some, or all, of the cost of producing inaccessible data, in other words, data that must be restored or otherwise manipulated to be usable, to the requesting party only if the responding party proves that the discovery request imposes an "undue burden";
- the burden of production is "undue" when it outweighs the likely benefit of the discovery taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues; and
- the cost of attorney and paralegal review of accessible data and of inaccessible data once it has been restored to a usable form will not be shifted from the responding party to the requesting party.

Applying these principles, the court imposed on UBS 75 percent of the $166,000 cost of restoring and searching backup tapes for the pertinent period and the remaining 25 percent on Zubulake. The court also ordered UBS to pay the $107,000 in attorney and paralegal fees for document review. The court's decision to impose any cost on Zubulake was driven largely by her substantial income while working at UBS ($650,000 annually) and by the substantial damages that she sought to recover (allegedly exceeding $15 million), facts that will not be present in most employment discrimination lawsuits.

The court also provided important guidance concerning a business' duty to preserve records. In ruling upon Zubulake's request to sanction UBS, the court explained that a business must impose a "litigation hold" on routine data destruction in certain circumstances. This "duty to preserve" records arises at a minimum when a business receives notice that a formal administrative or judicial proceeding has been filed, and even sooner if the business has reason to believe that litigation is

See ***Retention****, page 16*

Retention

from page 15

on the horizon, for example upon receipt of a demand letter.

This duty to preserve does not extend to every document and bit of data. Documents and data in accessible format when notice is received, or created thereafter, must be retained only if prepared by or for those employees who will be the "key players," in other words, the principal witnesses in the litigation, or if the data is or will be relevant to the litigation. The willful, or even negligent, destruction of evidence subject to the duty to preserve could result in an "extreme sanction." In particular, the court could instruct the jury to draw the adverse inference that the party who destroyed the relevant evidence did so out of a realization that the evidence was unfavorable, raising a virtually insurmountable barrier for the target of the instruction.

Elements of an Effective Data Retention and Destruction Policy

With the principles enunciated in the *Zubulake* case as a backdrop, the starting point for controlling the monetary and nonmonetary costs of data retention, retrieval, and destruction is an effective data retention and destruction policy. This policy should be drafted before litigation is on the horizon. The legitimate business objectives underlying the policy's development should be carefully documented to rebut any future charge that the policy itself is a fig leaf for the willful destruction of relevant evidence.

To further safeguard the business against a charge of improper document destruction and to reduce the cost of electronic discovery, the policy should achieve the following:

1 List all document-retention periods established by statute or regulation. These retention periods will vary substantially based upon the sector within which a business operates and the types of records involved. Securities brokers and dealers, for example, are required to retain all business-related communications for three years, the first two years in an accessible format. Trucking companies must retain the results of employee alcohol tests for up to five years. All businesses must retain federal payroll tax records for at least four years from the date the tax is paid. Each business should carefully research and catalog all applicable statutory and regulatory retention requirements and comply with them.

2 Establish additional retention periods. Categories of information not subject to a statutory or regulatory retention period should be subjected to a specified retention period consistent with business imperatives. E-mail in accessible format, for example, should be subject to a short retention period — perhaps 30 days — unless earmarked for longer retention because of business needs.

Each business should carefully research and catalog all applicable statutory and regulatory retention requirements and comply with them.

3 Provide for the routine destruction of documents and data. Data and documents should be routinely destroyed upon expiration of a statutory or regulatory retention period or expiration of the period mandated by the policy. Backup tapes should be recycled on a regular schedule. Regular recycling will significantly reduce the need to restore and search inaccessible data, the most costly aspect of electronic discovery. IT personnel should ensure that backup tapes containing data subject to a statutory or regulatory retention period are destroyed only after the retention period has expired.

4 Encompass all storage media. Potentially discoverable data may reside on any form of storage medium, including network server, local hard drive, laptops, handheld devices, optical disk storage, and backup tape. The policy should expressly apply to all of these media and specify variations in retention periods, if any, based upon the type of storage medium. For example, backup tapes containing e-mail for disaster recovery purposes typically should be retained for a longer period than e-mail saved to the network server or a local hard drive.

5 Suspend routine destruction to the extent necessary when

Steps for Reducing Document Recovery Costs

- ❑ List all document retention periods established by statute or regulation.
- ❑ Establish additional retention periods.
- ❑ Provide for the routine destruction of documents and data.
- ❑ Encompass all storage media.
- ❑ Suspend routine destruction to the extent necessary when litigation is on the horizon.
- ❑ Classify data in a manner compatible with search capabilities.
- ❑ Segregate privileged communications and confidential business information.

litigation is on the horizon. Once notified of actual or anticipated litigation, a business should identify all records related to the key players and all other categories of records most likely to be implicated in the litigation. These documents should be preserved in accessible form to avoid the cost of restoration and retrieval from backup tapes. The "key players" should be instructed concerning the types of newly created documents that must be preserved. If the business can identify backup tapes that might contain relevant evidence, those tapes should be excluded from routine recycling. Doubt concerning whether to retain or destroy certain documents should be resolved in favor of preservation.

The steps listed above also will help reduce the cost of responding to requests for production of information by limiting the total universe of data that is potentially subject to discovery. The following additional steps can further reduce these potentially exorbitant costs:

- **Classify data in a manner compatible with search capabilities.** Under *Zubulake*, the responding party bears the entire cost of searching accessible data and presumptively bears the entire cost of searching inaccessible data on backup tapes that have been restored. Given the enormous quantities of data involved, the search for responsive documents, unless automated, will substantially increase the cost of production.
- **Segregate privileged communications and confidential business information.** Responsive documents generally should be reviewed before production to ensure that privileged communications and other confidential business information are not produced to the adversary. In complex commercial cases, the volume of responsive documents can be substantial, making this "privilege pull" a costly exercise. These costs can be avoided, or significantly reduced, if privileged communications and other confidential business information are segregated when stored.

Once the data retention and destruction policy has been drafted, it should be uniformly enforced throughout the organization.

Once the data retention and destruction policy has been drafted, it should be uniformly enforced throughout the organization. Uneven application of the policy — for example, permitting high-level employees to destroy data more frequently than provided under the policy — could support a charge that the policy was intended to camouflage bad-faith destruction of evidence. In addition, the business should ensure that all storage media assigned to departing and terminated employees are routinely examined upon the employee's departure. Records subject to a statutory or regulatory retention period, or to a "litigation hold," should be preserved. Records retained for business purposes should be moved to the appropriate storage medium. All other data stored by the former employee should be destroyed.

Conclusion

Unlike Laura Zubulake, most employee-litigants do not earn $650,000 annually or possess multi-million dollar damage claims. In other words, employers can expect to bear the entire cost of electronic discovery in most employment lawsuits. Employers can lessen the monetary burden of electronic discovery and substantially reduce the risk of severe, nonmonetary sanctions by implementing a data retention and destruction policy guided by the principles described above. ■

About the author

Philip Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., the national labor and employment law firm. His practice emphasizes advising employers on the full gamut of workplace privacy issues. Gordon also serves as Human Resources section editor for the *Privacy Officers Advisor*. He can be reached at (303) 575-5858 and pgordon@littler.com.

Privacy Officers Advisor Calendar of Events

IAPP Audio Conference Series

Stakeholder Engagement: The Value of Working with Privacy Advocates
July 27, 2004, 1 p.m. – 2:30 p.m. EDT
Beth Givens, director, Privacy Rights Clearinghouse
Tess Koleczek, CPO, E-LOAN
Ari Schwartz, associate director, Center for Democracy and Technology
Frank Torres, director of consumer affairs, Microsoft
Alex Fowler, co-director, National Privacy Practice, PricewaterhouseCoopers (moderator)

Thriving in a Regulatory Environment: Do Not Call Compliance, Productivity and Driving Revenue
August 5, 2004, 1 p.m. to 2:30 p.m. EDT
Katie Harrington-McBride, attorney, Division of Marketing Practices, FTC
Michael Hogan, general counsel, Harris Investors
Keith Fotta, CEO, Gryphon Networks

For an updated schedule and registration information visit:
www.privacyassociation.org/html/audio.html

IAPP/Ernst & Young KnowledgeNet Meetings

Boston, July 20, 2004, 11:30 a.m. – 1 p.m.
San Francisco, July 21, 2004, 11:30 a.m. – 1 p.m.
Chicago, July 27, 2004, 11:30 a.m. – 1 p.m.
Boston, September 22, 2004, 11:30 a.m. – 1 p.m.
Washington, D.C., September 29, 2004, 11:30 a.m. – 1 p.m.
San Francisco Bay Area, October 6, 2004, 11:30 a.m. – 1 p.m.
New York City, October 12, 2004, 11:30 a.m. – 1 p.m.
Chicago, November 10, 2004, 11:30 a.m. – 1 p.m.
Atlanta, November 18, 2004, 11:30 a.m. – 1 p.m.
Philadelphia, To be determined

knowledge net

For more information on KnowledgeNet, or for the next scheduled meeting in your area, visit:
www.privacyassociation.org/html/knowledgenet.html

Privacy & Data Protection 2004
July 21, 2004
on board the HQS Wellington
Embankment, London
For more information:
www.java-events.com

First Conference on Email and Anti-Spam
July 30-31, 2004
Mountain View, Calif.
For more information
http://www.ceas.cc.

Crypto 2004: The Twenty-Fourth Annual IACR Crypto Conference
August 15-19, 2004
University of California, Santa Barbara
Santa Barbara, Calif.
For more information:
http://www.iacr.org/conferences/crypto2004.

Data Protection Compliance for Companies Doing
Business in Europe
September 8, 2004
Trinity House, Tower Hill, London, U.K.
For more information call:
+44 (0) 207 287 2561

26th International Conference of Data Protection and Privacy Commissioners
September 14-16, 2004
Wroclaw, Poland
For more information:
http://www.giodo.gov.pl/252/j/en/

IAPP Privacy and National Security Colloqium
Sponsored by Gray Cary
September 30, 2004
Washington, D.C.
For more information:
www.privacyassociation.org

IAPP Entertainment & Privacy Colloqium
October 7, 2004
Los Angeles, Calif.
For more information:
www.privacyassociation.org

IAPP Privacy and Data Security Academy & Expo
October 27-29, 2004
New Orleans, La.
For more information:
www.privacyassociation.org/html/academy.html

To list your privacy event in the Privacy Officers Advisor, *e-mail Mike Spinney at spinzo@earthlink.net.*

The Truth about Age Screening

Shai Samet, Esq.

COPPA Corner

When businesses think about the Children's Online Privacy Protection Act, or COPPA, the first thing that often comes to mind is *age screening*; that is, what steps should my organization take to identify the age of the Web site visitor prior to the collection of personal data from that visitor. After all, if COPPA regulates the collection of personal data from children under 13, it would seem only logical to implement an age gate at all data entry points and screen for underage users.

Given that, and what seems to be the underlying purpose of COPPA (*i.e.*, to give parents greater control over the collection and use of their children's data online), it may be surprising to hear that COPPA does not require age screening at all. In fact, the law itself does not even make mention of age screening, let alone impose any sort of age screening requirement.

Why the omission? Because when the Federal Trade Commission implemented the COPPA rule, their intention was not to encourage companies to roll out age fields in the masses and avoid collecting data from children entirely (as many have done) but rather to ensure that companies that do collect data from children — whether because their Web site appeals to children or because they have actual knowledge that many visitors are under 13 — do so responsibly and in accordance with the rule's parental notice and consent requirements.

Most Web sites on the Internet today are *general-audience* Web sites, meaning they appeal to people of all ages and are often too sophisticated for children to understand and use. This fact is important because when taken with the statements about COPPA above, the result is that general-audience Web sites have no obligation to investigate the ages of their visitors prior to data collection (*See* preamble to COPPA rule at p. 59,892).

In fact, these sites are much better off not asking for age information, lest they come into contact with data about children that they would not have otherwise known about and for which they are now responsible to handle in accordance with COPPA.

Interestingly, this principle of age screening, or lack thereof, also holds true with respect to Web sites that *are* directed to children, albeit for a very different reason. COPPA implies that companies that operate Web sites directed to kids must assume that all of their visitors and hence registrants are under the age of 13. This means that if these companies desire to collect personal data from their online customers (who are presumably children), they must refrain from requesting age information and instead take all of their visitors through a parental consent process, regardless of the actual age of the user.

While this may impose a burden on young-hearted teenagers who use the site, or parents who come to the site to register on their child's behalf, to ask for age information under these circumstances would only be counter to the spirit of the law.

So when does the predominant practice of age screening really apply? When your Web site is on the border line, when your product appeals to teenagers and children alike, or any other time a large percentage (although not all) of your Web site customers are under 13 years old (*See* COPPA FAQ No. 39 at http://www.ftc.gov/privacy/coppafaqs.htm).

But be sure that if you do solicit age information for this purpose, you do so in a way that does not encourage children to lie about their age. For example, stay away from statements on the registration page like, "You must be at least 13 years old to register," or use techniques (such as a session cookie) to prevent Internet-savvy children from clicking back and entering an older age. After all, not taking these measures would only defeat the purpose of age screening, that is, when the requirement exists in the first place. ■

About the author

Shai Samet is the chief privacy officer for Referral Technology Inc., a leading online referral source that generates consumer leads in the automobile and home improvement industries through its award winning Web site, www.PriceQuotes.com. He previously served as director of the Entertainment Software Rating Board's Privacy Online Program, where he advised more than 30 entertainment software publishers on compliance with privacy laws such as COPPA, the EU safe harbor, and industry best practices. Shai can be reached at shai@pricequotes.com or (917) 359-7585.

Age Gates and COPPA

When you should, and should not, implement an age gate to comply with COPPA:

- **General-audience or mixed-appeal Web sites** should *not* implement an age gate. These sites should assume that their visitors are 13 and older, unless they are given notice to the contrary.
- **Sites directed to children** should *not* implement an age gate. They should assume that their visitors are under 13 and take all visitors through the required parental consent process unless an exception to parental consent applies.
- **Sites directed to teenagers and children should** implement an age gate and allow children under 13 to register with the appropriate parental consent.

Haiku Do You?

You could become the IAPP's 2004 Haiku Champion!

Win a Mini-iPod!

How to Haiku Haiku is meant to capture the essence of a subject in simple form, placing great importance on word economy. Construct a privacy-focused poem formed in three unrhymed lines containing five, seven, and five syllables respectively, as in the following example:

Me, privacy pro?
Acronym professional
Is more accurate

How to Enter Mail your entries (you may enter more than once) by August 1 to the IAPP, 266 York Street, York ME 03909, or e-mail them to jackie.jones@privacyassociation.org.

The winner will be announced in the September edition of the *Privacy Officers Advisor*. Runner-up entries will be published over several months.

iapp
international association of privacy professionals