Privacy Officers Advisor

POA The official monthly newsletter of the Privacy Officers Association

June 2001 Editor: Marilou M. King, Esq. Volume 1, Number 9

POA Holds First Annual Meeting

Marilou King

The Privacy Officers Association held its First Annual Privacy & Data Protection Summit on May 2–4, 2001. More than 350 corporate privacy officers, security officers, government officials, academics, attorneys, and consultants gathered in Arlington, Va., across the Potomac River from the Capitol, to exchange views and learn from one another about the privacy and data protection laws and policies in business and government in the United States and the European Union. The participants came from the following industries: health care, financial services, e-commerce, government contracting, and telecommunications. No matter their role or their industry, the participants were united in their desire and need to understand emerging privacy and data security issues and the ever-growing regulatory restrictions on business practices. Compliance was the operative word. Participants were surprised to learn that many compliance initiatives are common to different industry segments. The medical privacy rule, which was made effective by the Department of Health and Human Services on April 14,

*See **Summit**, page 7*

The Costs of Internet Privacy Protections

Peter P. Swire

Recently, Robert W. Hahn, a resident scholar of the American Enterprise Institute, released a study entitled "An Assessment of the Costs of Proposed Online Privacy Legislation" (www.actonline.org/press_room/releases/050801.asp). The study, sponsored by the Association for Competitive Technology, was reported on May 8 in the *New York Times* and elsewhere as estimating costs of $30 billion or more to comply with possible Internet privacy legislation. I believe that based on the study's own assumptions, there are serious analytic flaws in the conclusions. The estimates are far too high, and I believe that they should not be relied upon for decision-making by policy makers or the private sector.

My concerns with the Hahn study fall into two categories. First, the study does not adequately address the key issue for any cost estimate — what is the baseline against which the cost comparison is made? In measuring the difference between a world with legislation and one without legislation, what behavior do we expect in

*See **Costs**, page 2*

Can Data Profiling Be Discriminatory?

Thomas B. Kleyle

Most of us are familiar with the following scenario. In the weeks after moving into a new home a homeowner begins receiving solicitations for life insurance without making any inquiry into purchasing insurance. The same homeowner also begins receiving a deluge of unsolicited offers of home equity loans. This pattern is repeated on a daily basis across the country as companies attempt to streamline their sales offers to customers that they believe have an immediate need or desire for their product.

Companies refer to this as targeted marketing and believe that, when properly executed, it is an effective process for both the company and the customer. Companies benefit by sending solicitation materials only to potential customers who have shown signs that they may be interested in purchasing a particular product or service. This reduces the marketing costs to the company by removing from its mailing lists potential

*See **Discriminatory?**, page 4*

This month ...

Privacy Officers Advisor

Editor
Marilou M. King, Esq.
McDermott, Will & Emery
Phone: 202/756-8244
E-mail: mking@mwe.com

Section Editors

Health:
Cindy Nichols, HCA Healthcare
cindy.nichols@hcahealthcare.com

Government Contracts:
Craig Holman, Holland & Knight
caholman@hklaw.com

Internet:
Ray Everett-Church, PrivacyClue
ray@privacyclue

Financial Services:
Patrick Sullivan, Guardent
patrick.sullivan@guardent.com

Telecommunications:
Douglas McCollum, CoreFacts
dmccollum@corefacts.net

To subscribe, call:
800/638-8437

For customer service, call:
800/234-1660

Publisher
Jane Garwood

Executive Director
Jo Gulledge

Managing Editor
Steve Larose

Editorial Production Manager
Eric Myers

Production Editor
Douglas M. Burnette

Advertising Sales
Steve Kavalgian, Mill River Media, LLC
Phone: 203/255-9150, e-mail: mehran32@aol.com

Privacy Officers Advisor (ISSN: **1532-1509**) is published monthly for $199 per year by Aspen Publishers, Inc. at 7201 McKinney Circle, Frederick, MD 21704. Telephone 301/417-7500.

Postmaster: Send address changes to: Privacy Officers Advisor, 7201 McKinney Circle, Frederick, MD 21704.

Subscription price: $199 per year, plus postage, handling, and appropriate state sales tax.

Business and circulation: Fulfillment Operations, Aspen Publishers, Inc., 7201 McKinney Circle, Frederick, MD 21704.

Requests to reprint: Permissions Department, Aspen Publishers, Inc., 200 Orchard Ridge Drive, Gaithersburg, MD 20878. Phone: 301/417-7638.

Costs

from page 1

the world without legislation? Without a clear picture of the world without legislation, we cannot assess the extra cost of the world with legislation.

Second, the assumptions in the study drive toward substantially overstated costs. The study assumes that small sites would spend as much as large sites to comply. It assumes too many sites. Each site would have to achieve unrealistically demanding standards. And each site is assumed to spend the large premium needed for a customized first-of-a-kind system, with no packaged software and no learning from experience.

The Importance of Defining the Baseline

The cost of privacy legislation is the difference between what industry would do in the absence of a law and what it would do if the law were enacted. As the Hahn study points out, Internet companies have made significant efforts in the privacy area. For instance, almost all significant Internet companies today have a stated privacy policy, and violations of the stated policy can lead to enforcement actions at the state and federal level. The cost of legislation is thus the extra, or incremental, cost of the new legislation.

There are many reasons that Internet companies address privacy in the absence of federal legislation. For instance, they do so to promote consumer confidence in Internet transactions or to comply with legal standards for customers outside of the United States. Importantly, companies take many measures that are simply good business practice. For instance, any responsible company has a firewall for its Web site. If a law were passed requiring a firewall (and I am not advocating such a law in making this point), then the cost of the legislation might be almost zero — most companies would already be taking that action.

The entire estimate of cost thus depends crucially on the baseline against which cost is measured. If companies are taking a level of appropriate action under self-regulation, as Hahn seems at some points to suggest, then a law setting that same standard would have low or no compliance costs. On the other hand, if companies are failing to follow basic good business practice, such as failing to have fire walls, then it is wrong to blame the law for the cost of the fire walls. The fire walls should be seen as part of the cost of doing business and not some extraordinary burden imposed by legislation.

Unfortunately, in the Hahn study, the baseline is not defined clearly enough. The result, I believe, is that the likely costs of legislation are overstated. The study at some points seems to support the view that the Internet industry has already taken substantial and effective steps to provide privacy protection. Yet the expenses already incurred are never netted against the gross estimates of cost. It is as if one reports the cost of building a house without subtracting out the cost of a foundation and a couple of walls that are already in place.

The Study's Assumptions Lead to Substantially Overstated Cost Estimates

The study fails to distinguish between large and small sites, assumes an excessive number of sites, uses unrealistically demanding and expensive standards for each site, and assumes that all compliance will be customized rather than having any reduction in cost after the first company has complied. These assumptions have led to an overstated estimate of compliance costs.

Large and Small Sites Are Different

The study surveys consultants about how much it would cost for a large site to comply, for a site with at least 100,000 current customers and the capability to scale to millions of customers. The survey finds an average cost per site of $100,000 (more on that figure below). But that cost is based entirely on the estimated cost for building a complex large site. As the study itself discusses, it is unreasonable to expect that a small Internet

site will spend $100,000 for privacy compliance, and the cost would be much lower for a small site even though the survey failed to ask for the difference in cost.

Too Many Sites

The study's $30 billion estimate, called "conservative" in the study, cannot be defended on the basis of the study itself. That estimate assumes that 360,000 sites do the expensive $100,000 compliance solution. But the study itself also says that there is a grand total of only 94,000 "medium to large" commercial Internet sites. The extra 246,000 sites are "small" sites, and the estimate for a site serving millions of customers simply does not apply. Each of these "small" sites, however, was counted at the $100,000 per site compliance rate.

The study's lowest cost figure is $9 billion. That figure assumes that every single large *and medium* site spends the full $100,000 per site for compliance. (The study defines size based on the company size, with "large" having over 500 employees, "medium" 100 to 500 employees, and "small" fewer than 100 employees. Some "large" companies may not have consumer sites scalable to millions of customers, so they may not have "large" sites. Some "small" companies, but proportionately likely not many, may have large sites that are designed to serve millions of customers.) This $9 billion estimate thus assumes too many sites for at least two reasons. First, it assumes that medium-sized sites will have to pay the same as large sites. Second, it assumes that the medium and large sites do not already have significant self-regulatory programs in place to provide privacy protections. Yet many of these larger sites have already instituted significant privacy programs. The cost of compliance should thus be reduced to take account of the measures already in place, and this was not done in the study.

Unrealistically Strict Criteria

The study asks consultants to estimate what it would cost to build a new system that complies with a set of criteria. Defining those criteria is crucial. If the criteria are easy, then costs will be low. For instance, it would cost little if the law says: "Mention the word privacy on your web page." If the criteria are strict, then costs will be high. For instance, it would cost a great deal if the law says: "Design a state-of-the-art system that handles personal information in complex new ways that have never been done before."

The problem is that the study assumes criteria that resemble the latter. Two examples from a longer list give the flavor. First, the study assumes that every time personally identifiable information (PII) is sent to any third party, the Web site must have a complete tracking of all of its PII about that customer. If the Web site sends out PII about that customer to someone the next day, it must keep a complete file of the changed PII that exists on that second day. This sort of time-and-date stamping of every item of information about every customer is either rare or unknown in the industry and is unlikely to become law. Yet that is the system that the study assumes every Web site will have to build. A second example is that the study assumes that the customer access rules will be significantly stricter than I believe anyone has seriously proposed legislating. In defining the access requirements so strictly, for instance, the study assumes not only that individuals will get online access to a complete log of every time their PII has gone to a third party but also that customers will also gain access to the complete content of what is transferred to the third party. Again, this sort of time-and-date stamping of the content that is transferred is either rare or unknown in the industry.

It is thus no surprise that the consultants estimated that it would be expensive for each Web site to comply. The criteria included features that have not been implemented in the industry and not seriously contemplated in legislation. As the consultants imagined what it would cost to build these new types of systems for the first time, they correctly stated that it would be very expensive. But the $100,000 average estimated cost is a reflection of an unrealistically strict

*See **Costs**, page 4*

POA

Privacy Officers Association

1211 Locust Street
Philadelphia, PA 19107

Phone: 800/266-6501 or 215/545-8990

Fax: 215/545-8107

E-mail: information@privacyassociation.org

Web: www.privacyassociation.org

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

Costs

from page 3

set of criteria, rather than of the cost of compliance with likely legislation.

All Compliance Is Customized and There Is No Learning from Experience

The survey asked consultants to estimate how much it would cost to build this complex, strict system for the first time. Their estimate of $100,000 per site for building a new system was then used as the average cost of compliance per site. The over $30 billion estimated total cost assumed that 360,000 sites (large and small) would each build a new system from scratch for that $100,000 per site.

But that is not the way that software works today. According to the study's figures, most of those 360,000 sites are small or medium sites. These sites will not ask expensive consultants to write entirely new one-of-a-kind software. Instead, small, medium, and many larger sites will buy software packages. Implementation may include a moderate amount of tailoring for a particular company. But the cost of that tailoring is much less expensive, often by an order of magnitude, than writing software from scratch. The incremental cost of compliance will further be reduced because privacy compliance will likely be undertaken as part of a broader upgrading of a site, of the sort that is often done in the rapidly changing Internet environment, rather than as a stand-alone cost item.

Put another way, the first system of a new type costs far more to build than the 360,000th. Experience gained in early systems makes it far less expensive to build later systems. Even if Congress surprises everyone by requiring every one of the unrealistically strict criteria that the study assumed, later systems will cost much less than the $100,000 that the study uses. And, Congress will not likely impose those criteria, so the cost of actual legislation will be even less.

Conclusion

I have written this detailed analysis of the study because of my concern and belief that it will be irresistibly tempting for critics of privacy legislation to quote the $30 billion, or even the $9 billion, estimate as though these are realistic figures. However, the study does make the correct point that badly drafted legislation, in privacy as in other areas, can impose substantial and undesirable costs. If Internet privacy legislation is enacted, then it should be based on careful attention to how principles such as notice, choice, access, security, and enforcement would work in practice. In seeking to discern useful information flows from invasions of privacy, policy makers need to rely on more realistic estimates of the effects of legislation than I am afraid this study provides. ■

About the author ...

Peter P. Swire is professor of Law at the Ohio State University. In the 2001-2002 academic year, he will be a visiting professor of law at George Washington University. From 1999 until early 2001, Professor Swire served as the first chief counselor for privacy in the U.S. Office of Management and Budget. During his tenure there, he worked extensively on the regulatory impact statement for the HIPAA medical privacy rule. He can be reached at pswire@main.nlc.gwu.edu or through his Web site at www.osu.edu/units/law/swire.htm or 301/213-9587. The views expressed are those of the author. The editors of the newsletter welcome thoughtful responses.

Discriminatory?

from page 1

customers who are unlikely to purchase products or services. Customers benefit by receiving solicitations for products and services that fit their needs, while presumably avoiding being deluged by marketing solutions in which they have no interest.

This target marketing, enabled by complex data modeling and customer profiling techniques, is intended as mutually beneficial for both companies and consumers. Personalization technologies that enable companies to move closer to one-to-one marketing are effective in developing highly sophisticated pictures of consumer interests and preferences to which companies can direct efforts to build lasting customer relationships. Yet, while data profiling and targeted marketing possess significant opportunities to reduce marketing costs and to cater to customer preferences, there are potentially negative uses or impacts to this type of customer segmentation.

Companies can determine who receives solicitations for products and services based upon the results of often-complex analysis of customer demographics and past purchasing habits. This analysis involves merging a vast array of personal data such as location, financial, and lifestyle information into a single snapshot of a customer with a propensity to purchase a company's services. Taken further, this analysis may be used to target customers to receive a certain class or type of product. The advanced algorithms of the data modeling enable a projection of which products or services the customer will want or will be likely to purchase. As a result, a customer may receive a very different solicitation from their new neighbor. The reasons for the differences in products and services offered may reside deep within the algorithm and may not be readily recognizable to either the customers or the companies.

Inherent in the benefits of targeted customer marketing is the ability to select the customers that a company markets to with a relative degree of precision. What is beginning to concern privacy advocates is the possibility that this same process can be used, either explicitly or implicitly, to determine which customers a company decides to exclude from its marketing campaigns. In many industries excluding customers from