

PRIVACY & DATA SECURITY LAW JOURNAL

VOLUME 5

NUMBER 2

FEBRUARY 2010

HEADNOTE: DEVELOPMENTS	
Steven A. Meyerowitz	97
FEDERAL TRADE COMMISSION CONTINUES TO EXPLORE CONSUMER PRIVACY PROTECTION MEASURES	
Dana B. Rosenfeld and Megan L. Olsen	99
NEW ORGANIZATIONAL GUIDELINES CHANGES: INDEPENDENT MONITORS ARE BACK IN VOGUE AND YOU BETTER KNOW WHEN YOUR OLD E-MAIL IS DELETED!	
Nathan Muyskens	104
FINRA ISSUES GUIDANCE ON SOCIAL MEDIA WEB SITES	
Amy N. Kroll and Paul M. Tyrrell	109
FINCEN EXPANDS ACCESS TO SECTION 314(A) INFORMATION REQUESTS	
Maureen Young and Paul M. Tyrrell	117
THE NEW MASSACHUSETTS DATA SECURITY REGULATION: WHY IT WILL CHANGE AMERICA'S PRIVACY AND SECURITY LANDSCAPE	
Eduard F. Goodman	124
COMPREHENSIVE NEW MASSACHUSETTS DATA SECURITY REGULATION WILL AFFECT MANY NATIONAL BUSINESSES	
John Kennedy and Vivian Polak	136
LITTLE ADO ABOUT MUCH: RECENT U.S. FEDERAL DATA PRIVACY DEVELOPMENTS	
Satish M. Kini	141
FTC SETTLEMENTS SPOTLIGHT HAZARDS IN THE U.S.-EU SAFE HARBOR	
Amy E. Worlton	148
ENFORCING A CIVIL JUDGMENT AGAINST A PERSON PROTECTED BY THE WITNESS PROTECTION PROGRAM	
Victoria Prussen Spears	151
NINTH CIRCUIT RULING HIGHLIGHTS PERSONAL RISKS TO COMPANY EXECUTIVES FACED WITH INTERNAL INVESTIGATIONS CONDUCTED BY CORPORATE COUNSEL	
Steven A. Meyerowitz	159
INTERVIEW: RANIA V. SEDHOM DISCUSSES GLOBAL DATA PRIVACY AND SECURITY ISSUES	178
PRIVACY & DATA SECURITY LAW DEVELOPMENTS: 2009 ROUNDUP AND 2010 FORECAST	
L. Elise Dieterich, Wendy M. Creeden, Kathy L. Cooper, and Ronald P. Whitworth	188

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

MANAGING EDITOR

Adam McNally

SENIOR EDITOR

Catherine Dillon

BOARD OF EDITORS

Michael P. Carlson

Faegre & Benson LLP

Michael Cohen

Wolf Block Schorr & Solis-Cohen

V. Gerard Comizio

Paul, Hastings, Janofsky & Walker, LLP

Michael A. Gold

Jeffer Mangels Butler & Marmaro LLP

Andrew J. Graziani

Hogan & Hartson L.L.P.

Benjamin S. Hayes

Accenture

Gary A. Kibel

Davis & Gilbert LLP

Satish M. Kini

Debevoise & Plimpton LLP

Sharon R. Klein

Pepper Hamilton LLP

Rodney D. Martin

Warner Norcross & Judd LLP

Catherine D. Meyer

Pillsbury Winthrop Shaw Pittman LLP

Adam C. Nelson

IBM Security & Privacy Services

Jeffrey D. Neuburger

Proskauer Rose LLP

Scott M. Pearson

Stroock & Stroock & Lavan LLP

Kenneth Rashbaum

Sedgwick, Detert, Moran & Arnold LLP

William M. Savino

Rivkin Radler LLP

Rania V. Sedhom

Buck Consultants, LLC

Gregory P. Silberman

Kaye Scholer LLP

Liisa M. Thomas

Winston & Strawn LLP

Christopher J. Volkmer

Volkmer Law Firm LLC

Christopher Wolf

Proskauer Rose LLP

COLUMNISTS:

LANDMARKS

Victoria Spears

Victoria Prussen Spears, P.C.

THE STRATEGIC FRONT

Martin Abrams

Hunton & Williams LLP

TRADE SECRETS

Jeffrey W. Post

Fredrikson & Byron P.A.

The PRIVACY & DATA SECURITY LAW JOURNAL is published monthly by Sheshunoff Information Services Inc., 805 Fifteenth Street, N.W., Third Floor, Washington, D.C., 20005-2207. Copyright © 2010 ALEXESOLUTIONS, INC. All rights reserved. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For permission to photocopy or use material electronically from the *Privacy & Data Security Law Journal*, please access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For subscription information and customer service, call 1-800-572-2797. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 10 Crinkle Court, Northport, NY 11768, smeyerow@optonline.net, 631-261-9476 (phone), 631-261-3847 (fax). Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. Although the utmost care will be given material submitted, we cannot accept responsibility for unsolicited manuscripts. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher. POSTMASTER: Send address changes to the *Privacy & Data Security Law Journal*, Sheshunoff Information Services Inc., 805 Fifteenth Street, N.W., Third Floor, Washington, D.C., 20005-2207.

Interview:

Rania V. Sedhom Discusses Global Data Privacy and Security Issues

The *Privacy & Data Security Law Journal* recently spoke with Rania V. Sedhom, an attorney and principal with New York-based Buck Consultants. Ms. Sedhom, who can be reached at Rania.Sedhom@buckconsultants.com, addressed many timely, important privacy issues facing companies both in the United States and abroad.

WHAT IS PRIVACY AND DATA SECURITY?

Q: Let's begin with some basics: what specifically does "data privacy and security" refer to, and why is it important?

A: Data privacy and security is a broad term relating to everything relative to data gathering, storing, destroying, and sharing. When an organization ensures data privacy, it is ensuring that people who are not authorized to see private data cannot examine it.

Data privacy and security is of crucial importance for a variety of reasons. Above all, in the United States data privacy is becoming a fundamental right, and organizations running afoul of sound privacy standards leave themselves vulnerable to litigation. Moreover, American companies doing business on a global level must ensure that its data privacy and security protocols are both effective and sound. Of course, there are also associated ethical and competitive concerns. However, actually determining what information demands privacy protection is a difficult matter.

HOW TO DETERMINE IF CURRENT PRIVACY POLICIES ARE ACCURATE

Q: Building on that, how can a company determine if its current privacy policies are adequate?

A: The process should begin with an audit, or as-is assessment, to evaluate the company's current policies. At this early stage, the objective is determining if the current policies are administratively sound, reflect the current organizational needs, and adhere to the applicable laws. A good way to begin conducting an as-is assessment is by comparing day to day staff operations with the will of management and note any gaps. Often times, companies will realize that the procedures they believe are being followed actually are not.

Whether or not an organization is prepared to undertake an internal audit of its data privacy and security procedures, certain questions must be answered. These questions include:

- What do you need to protect? For example, are you only protecting personal employee or client/customer information, or do you also have trademark agreements or even customer and vendor lists to protect?
- Where do you operate geographically, and where do you plan on operating in the next 12 months? Different regions have different laws.
- How important is risk management to your company?
- How do you balance the rights of your employees versus the rights of your company?
- What is your organization's "threshold of pain," in terms of how operationally intensive and rigorous a policy you are willing to implement?
- Who in your company will be responsible for data privacy oversight?
- When was the last time management and employees were trained on matters of data privacy and security, if ever?
- How, if at all, do you monitor employee and vendor safeguarding of private data?

RIGHTS OF EMPLOYEE VERSUS RIGHTS OF THE COMPANY

Q: You mentioned the rights of employees versus the rights of the company. Please explain.

A: Companies should take into consideration individuals' concerns over the use of what they consider to be private data or information. This is where the needs of the individual and the needs of the company can diverge, because what a person may consider private, an organization may consider as information eligible for selling or sharing. Fortunately, this does not boil down to guesswork: there are global and, in the U.S., federal and state privacy laws that define these rights. But, they are not always easy to interpret, which is why organizations so often seek outside assistance.

WHAT INFORMATION IS LEGALLY PROTECTED?

Q: What items are subject to legally mandated privacy restrictions?

A: It is a long list, including:

- Arrest records;
- Bank records;
- Data banks;
- Employment records;
- Insurance records;
- Mailing lists;
- Medical records;
- Privileged school records;
- Social security numbers and other government issued identification numbers;
- Tax records;
- Phone solicitations; and
- Wiretaps.

Some of these are fairly obvious; companies know they must keep social security number private. But, others are not so obvious. Obvious or not, they come with significant and serious legal restrictions.

The list of what is considered private personal information also changes with geography. For example, telephone numbers are considered protected information in France.

RESTRICTING ACCESS TO PROTECTED DATA

Q: So, how do you restrict access to a company's data?

A: There are entire systems and structures designed to do just that. One way to help keep data private is to have adequate data access controls in place to protect information from unauthorized viewing and alteration. I often urge companies to bear in mind the “GAP” principle:

- Guidelines for protecting confidential data should exist and be readily available to employees;
- Applicable privacy laws and regulations must be adhered to; and
- Policies should be detailed and audited for risk management.

Another concern is password administration. One common approach is to provide passwords — or to allow certain employees to choose their own passwords — to anyone who may view or use private data. As an important aside, however, you've got to make sure to choose a *strong* password: simply selecting the word “password” or your oldest child's first name does not go very far in creating a password that is difficult to hack.

I always advise companies to make sure their employees follow the “CREEP” rule. CREEP is just an acronym to remind users to make sure that the creep (the hacker) has a difficult a time as possible breaking their secret code:

- Changing passwords periodically must be required;
- Repeat characters infrequently;
- Employees must choose a specific number of characters
- Easily guessed passwords are prohibited; and
- Passwords may not be used more than once per year.

Another area to address is database and network administration, which helps control the security of confidential information shared on multiple interfaces by multiple users. It is crucial that organizations establish encryption policies for handling this type of information, whether it is being transmitted on a laptop or cell phone or over a fax machine or PDA.

One final area I'll mention is data storage and destruction. Remarkably, this is the stage where security breaches often take place because of carelessness. But, it is as important to identify and control sensitive information at the disposal phase as it is at any other time; just because the information is being destroyed does not mean it is not potentially sensitive and private.

BUSINESS ADVANTAGES TO PROTECTING DATA

Q: You've talked a lot about the legalities of privacy, but what about business advantages to protecting data; are there any?

A: Absolutely. The public has never been more knowledgeable or interested in the information security practices of the companies they do business with, and that holds true on a global basis. I'm not saying these practices are the ultimate arbiter of purchasing decisions, but they definitely play a part. And, of course, there are obvious financial ramifications to protecting institutional knowledge and proprietary product data.

DATA PRIVACY ABROAD

Q: You mentioned global markets, so let's step away from the United States for a moment. Are data privacy and security matters dealt with differently in other countries?

A: That is actually quite an important question as more companies expand from the U.S. into foreign markets. And the answer is, yes, international privacy laws differ quite a bit from those in the United States, both in terms of scope and how they are applied. In fact, there's little global uniformity which makes it that much harder to ensure data privacy and

security globally.

One exception is the European Union (“EU”): the laws differ in some ways from those in U.S., but they’re generally consistent within EU countries.

As in the U.S., EU law considers data protection to be a fundamental human right. This goes all the way back to Germany in 1938, when its federal constitutional court recognized a right to what it referred to as “informational self-determination.” That same right is recognized throughout the other 25 EU countries. Actually, the EU was the first legal system in the world to create a data privacy anthology covering various sectors and industries.

Featured elements of EU data protection law include a defined minimum level of data protection for individuals and no restrictions on data transfers among the 25 member countries. That said, there is little synchronicity among each country’s individual data protection laws. That is a critical factor to consider when operating in the EU, and it makes it a good idea for U.S. companies with global presence to consider adopting a safe harbor plan.

SAFE HARBOR PLAN

Q: What are the basic elements of this sort of plan?

A: The basic elements are fairly straightforward. First, it is important to conduct a company wide, as-is assessment to determine the state of the current data security protections. From there, a gap analysis should be conducted to identify any weaknesses in the current programs, and create new policies and procedures to shore up those weaknesses. This is also an important step in laying out an overall plan for data security in the company.

It is key, of course, for those who operate on a company’s behalf to be aware of and to understand those policies, so these new policies and procedures must be clearly communicated to employees, third party vendors, and affiliates. The whole point here is to educate them and ensure they recognize their accountability in complying with the new standards.

Finally, there needs to be a system in place for monitoring compliance and maintaining accountability.

CHALLENGES ENACTING A SAFE HARBOR PLAN

Q: That sounds straight forward enough. Are there any stumbling blocks to watch out for?

A: Yes, certainly. For starters, there is cost. The sort of safe harbor plan development I just summarized can be financially prohibitive for some companies. For that reason, some companies might decide that the as-is assessment simply will not elicit enough feedback to merit the expense. The deeper your assessment, the more it is going to cost. Some organizations prefer to deal with these matters on an ad hoc basis; they wait for something to go wrong and then identify and fix the problem at that point.

The upside to this approach is not committing the upfront investment. The potential downside, quite obviously, is that the company is only one data breach away from a huge disaster. So, proponents might refer to this approach as “sticking your toe in the water” rather than diving in. Others might consider it more akin to sticking your head in the sand.

Cost is far from the only challenge. Some organizations, especially larger ones, have a lot of trouble building internal consensus on the proper approach to a data security program. It is a topic nearly every part of the company weighs in on because it affects virtually all areas of operation, and each department tends to have their own ideas about how it should be approached. This is not an easy situation to rectify, for reasons ranging from turf battles to the fact that, as an example, marketing tends to speak a seemingly different language from IT. And legal has yet another way of speaking.

ADDRESSING THE CHALLENGES

Q: How do you revolve that challenge?

A: It typically takes a third party with expertise in both the law and consulting to step in and create a uniform policy everyone feels good about.

These policies must address privacy from a variety of angles and perspectives, and a qualified third party is simply better equipped to handle that than internal employees steeped in one discipline or business unit. This is not a one time deal; education such as training needs to happen regularly, maybe once or twice a year — it is an ongoing process.

INSTITUTING THE NEW POLICIES

Q: You mentioned the need to communicate to employees and other relevant constituencies. How do you best indoctrinate the company in new data privacy and security policies and procedures?

A: In a variety of ways, but it usually starts with training. Now, I do not know about you, but when I think of most training sessions I've been a part of, I can't help but instinctively stifle a yawn. So, you've got to find a way to make it interesting which, again, a qualified expert third party should be able to help you with. The stakes are too high for the training to not be taken to heart: the difference between "getting it" and "not getting it" can mean the difference between whether or not your company faces liability down the road.

But training only goes so far. Training only shows participation, not understanding or buy-in. Training does not give employees a stake in adhering to procedures or necessarily ensuring they understand the crucial role they play in maintaining security. For that reason, I suggest that in cases where employees and other third parties are trained, or when security related information is disseminated to them, they be asked to attest to the fact that they recognize their personal responsibility for regularly implementing every element of every data privacy policy the company maintains. This is essentially a part of everyone's job description.

CONSEQUENCES FOR DATA SECURITY BREACHES

Q: You've made clear the importance of data security. But, what are the specific ramifications here for companies that fail to comply?

A: Let's start from a place everyone can identify with: money. The Michigan Court of Appeals, in the case of *Bell v. Michigan Council 25*, awarded \$275,000 to a group of identity theft victims because the defendant had failed to implement proper procedures or safeguards to protect the personally identifiable information in its control. Even though the definition of proper procedures will likely transform over time, clearly the onus is on the companies that collect this data to stay one step ahead of the liability curve.

The truth is that data security breaches are a costly matter, because domestic and international laws grant a range of protections to consumers. These costs include the direct costs associated with handling the breach, and the downstream costs resulting from the repercussions of the breach. The numbers associated with data breaches, such as millions of records being lost, can make these costs quite significant.

TJX Companies, the discount retailing company, was involved in a very public data breach, and had to pay out \$65 million in settlements to Visa and MasterCard just for the cost of credit card replacement. It then settled a class action lawsuit for what appears to be north of \$100 million, although the exact figure was never released. Heartland Payment Systems, Inc.'s data breach may result in even higher costs!

That is just the tip of the iceberg. Data breaches can attract attention from government regulators, credit card associations, class action attorneys and even individuals — and the costs associated with this can add up rapidly. In fact, the Electronic Communications Privacy Act of 1986 provides for a *minimum* fine to offending entities of \$1,000 per person affected. That is how you wind up with situations like National Pharmacy Chains entering a \$2.25 million settlement with the U.S. Department of Health and Human Services over improper disposal of patient information; Choicepoint entering a \$15 million settlement with the Federal Trade Commission over the breach of 163,000 records; and Vodafone being forced by Greece's Data Protection Authority to pay a \$103 million fine for failing to protect its network from hackers who monitored just 100 mobile phone accounts. Unfortunately for Vodafone, one of those phones happened to belong to the Greek prime minister!

I could continue with more examples, but the point is clear: the financial ramifications of data breaches are potentially huge. Not even the government is immune to these ramifications: the Department of Veteran Affairs had to pay \$20 million to veterans affected by a data breach.

CLOSING REMARKS

Q: This all paints a rather vivid and pretty grim picture. Is there any positive to take from all of this?

A: Well, there's the old expression that forewarned is forearmed. Courts, and seemingly regulators, are beginning to recognize that data security breaches should not be viewed as strictly liability issues. If a company has reasonable policies and procedures in place, including sound protocols for communicating, training, and monitoring, it should be well positioned to plead "safe harbor" in the event of a breach, because in reality there is no 100 percent, fail-proof system to prevent data breaches.

This all the more underscores why organizations should take data privacy and security so seriously: the right policies and procedures significantly lessen a company's vulnerability to data breaches, and in the event there is a data breach, a company with strong policies and procedures in place are more likely to have a more satisfactory legal outcome.