Information Protection & Privacy - The New High Stakes Game

Eighth Annual Hospitality Law Conference
February 3-5, 2010
Houston, Texas

Chris Zoladz
Navigate LLC
(240) 475-3640
chris@navigatellc.net

Chris Zoladz
chris@navigatellc.net
240-475-3640
www.navigatellc.net

Chris Zoladz, CIPP, CISSP, CISA, CPA, CGFM is the founder of Navigate LLC, a consulting company focused on providing comprehensive strategic and tactical information protection & privacy consulting services to clients in the hospitality, government and healthcare sectors. Prior to founding Navigate in April 2009, Chris was the Vice President, Information Protection & Privacy at Marriott International, Inc. He created the function at Marriott in 1999 and had responsibility for global information protection and privacy strategy and operations to meet business needs and legal requirements in a cost-effective manner. Chris was also the co-leader for Marriott's *Payment Card Industry Data Security Standard* ("PCI DSS") compliance effort.

Prior to Marriott, Chris was the Mid-Atlantic Area Office Director of Information Systems Auditing & Security Services for Ernst & Young. Chris is a past-president and a founding board member of the International Association of Privacy Professionals (IAPP), was the recipient of 2006 IAPP Vanguard Award as the Chief Privacy Officer of the Year and is a frequent speaker on information protection and privacy topics at conferences.

TABLE OF CONTENTS

I. SCOPE OF ARTICLE

Protecting confidential and personally identifiable information[1] ("PII") from loss, theft or misuse is not a new concept. However, it is only over the past few years that this area has received considerably more focus as security breach laws and credit card company requirements have significantly increased the consequences when the security of certain information is breached. Information protection and privacy was historically not a high business priority but now it is a regular headline in major media and a mainstream focus area for many companies. As hospitality companies routinely deal with a considerable amount of PII, the importance of this topic is even greater than for some other companies. Customers and regulators expect more from companies than ever before. This paper describes customer expectations, business needs and major legal requirements that must be carefully balanced to not only protect the organization but also to enable management to meet their business objectives. The goal is to not only inform the reader of the key points in these areas but also to provoke and challenge the reader to identify opportunities for improvement at your company or the clients you serve. This document is not intended to be an exhaustive list of all applicable legal requirements. It was written for informational purposes only, and is not intended and should not be considered to be legal advice.

II. EVENTS SHAPING CONSUMER OUTLOOK

Over the past few years stories about data theft and losses have been told in numerous major print media and television news coverage. Since 2005, Privacy Rights Clearinghouse has maintained a chronology of data thefts and losses, including the number of affected individuals. As of December 2009, Privacy Rights Clearinghouse reports that there have been several hundred data breach and loss events since 2005 that resulted in over 340 million records containing PII being put at risk of misuse. These previously non-public events became a matter of public record with the advent of the U.S. State security breach laws that emerged in 2003 and will be discussed later in this paper. The result of the media coverage has been that the average consumer has become more knowledgeable about the risks that pertain to their information when entrusted to a hotel or other business, and also more concerned about the protection of their information. If your company's customer's PII is lost or stolen and misused, you likely have just lost a customer, perhaps forever. In addition, the customer will likely tell their story to friends and family and perhaps use a social networking website to share their experience where many customers or potential customers virtually hear the story.

[1] Personally identifiable information or "PII" is defined broadly as first and last name, or first initial and last name in combination with credit card number, driver's license number, social security number or other factual information specific to the individual.

III. CUSTOMER EXPECTATIONS

Meeting or exceeding customer expectations is at the heart of any successful business. In the hotel business for example, at a basic level this traditionally has meant following timeless principles such as ensuring the customer's room is ready upon arrival, the room is clean, everything in the room is in working condition, the bed is comfortable, the staff is responsive, etc. All of the "creature comforts" and personal service are certainly very important and determine if the customer will be a loyal customer. However, another facet of taking care of the customer is taking care of their PII. Customers entrust a significant amount of PII to hotels and other hospitality companies. This information typically includes name, address, email address, credit card information and preferences. In addition, hospitality companies understandably maintain historical information about the customer to personalize service delivery and marketing. Customers have the reasonable expectation that when they provide their PII the recipient will have appropriate controls in place to protect it from loss, theft or misuse. In addition, customers expect that their information will not be used for purposes other than for the purpose for which it was supplied, or that they at least will have a choice (i.e., opt-in or opt-out) before any information is repurposed. For example, it is common that information such as an email address that is collected during the reservation process will be used to send the customer not only a reservation conformation but also for sending marketing messages.

IV. BUSINESS DEMANDS

In these historic economic conditions, every hospitality company needs to focus on maximizing revenue and cutting costs. Regardless of economic conditions, focusing on customer facing revenue generating activities is always crucial. More specifically, attracting new customers and enticing existing customers to spend more money with your company is a core goal. One way to achieve this goal is through personalization of marketing and service delivery. The ability to personalize at either level is dependent on having the PII to act upon and then doing so intelligently. This is where a business risk is created. More PII equates to more potential risk of information theft or loss.

A. REDUCED STAFFING CAN RESULT IN INCREASED RISK

Many companies have reduced staffing over the past couple of years as a matter of business necessity. As a result, remaining staff usually are assigned additional responsibilities and experience more time pressure to complete assigned tasks. An unintended consequence of this action can be that controls and standard processes may get bypassed or compromised and place PII at risk. While staff reductions may be a necessity, the importance of adhering to appropriate internal controls to protect PII must be emphasized.

B. OUTSOURCING

As part of cost cutting measures or in the quest to enhance operational efficiency, many companies are using third party service providers to provide services such as payroll processing, benefits administration, website hosting, cloud computing[2] and a myriad of others. While cost savings and efficiencies can be realized, it is important that these service providers have appropriate information protection and privacy measures in place to properly protect the PII of your customers and/or employees that is entrusted to them. In addition, it is not uncommon for service providers to use contractors as part of their business operation. It is important that the appropriate information protection and privacy measures also be in place at these contractors. This can be a challenging area from two perspectives. First, there is the question of which security standard should be applied to assess the information protection and privacy measures in place at the service provider and any contractors and who will perform the assessment. Second, there is the question of how often (e.g., annually) this assessment would occur to ensure that the controls in place at the service provider and any contractors are still adequate and operating effectively. These challenges are directly compounded as the number of service providers and contractors increases. At large companies it is not uncommon that there would be dozens of service providers that are handling PII.

C. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The rise in credit card fraud has drawn the attention of the credit card companies, especially for the hospitality industry. Regulators also have been concerned about credit card fraud. In response to these growing concerns, and to put in place a meaningful self-regulatory process, the major credit card companies (Visa Inc., MasterCard Worldwide, American Express, JCB and Discover) have adopted a comprehensive information security standard that they believe, when complied with by all merchants and processors, will reduce the amount of credit card fraud. This comprehensive standard is called the Payment Card Industry Data Security Standard[3] (known as "PCI DSS" or "PCI" for short). PCI DSS was first published in 2004 and has been updated two times since its initial publication. The most recent update was issued in October 2008 and the next expected update will occur in October 2010.

---

[2] Cloud computing is a type of computing that is comparable to grid computing, relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing power (normally used by military and research facilities) to perform tens of trillions of computations per second. To do this, Cloud computing networks large groups of servers, usually those with low-cost consumer PC technology, with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. *Source: Webopedia.*

[3] A copy of the PCI DSS is available from the PCI Security Standards Council at http://www.pcisecuritystandardscouncil.org/.

Briefly, PCI DSS consists of approximately 250 detailed security requirements that apply to all computer applications and business processes that involve the collection, processing, storage or transmission of credit card data. While PCI DSS is not a law, it is a contractual requirement between the merchant and the merchant bank and is part of the credit card companies' operating rules and regulations. PCI DSS is a global and mandatory standard that applies to any merchant that accepts credit cards. PCI DSS can affect many of the operations at a company. For example, in a hotel, affected areas and business processes would include the Front Desk, Sales & Marketing, Food & Beverage and Accounting.

Non-compliance with PCI DSS can be very costly. A company that is non-compliant and/or suffers a security breach can typically expect:

- Monthly fines of $5,000 - $25,000 that will continue until PCI DSS compliance is achieved;
- A one-time fine and assessment from the credit card companies that can range from tens of thousands to hundreds of thousands and potentially even millions of dollars to cover the cost of reissuing cards and fraudulent charges on compromised cards;
- Potential inquiry and fine from the FTC and/or a State Attorney General;
- Lost business; and
- In the extreme case, the credit card companies reserve the right to prohibit the merchant from accepting their cards.

Clearly, the stakes of not being PCI DSS compliant or having a security breach are significant, and the risks must be mitigated. In addition, PCI DSS is also not a timeless standard. The Standard will change at least every 2 years as there are new technologies that pose new risks to credit card data and new techniques developed and used by credit card thieves and fraudsters that need to be defended against. Changes to PCI DSS may result in the need to upgrade systems even if the systems were previously deemed to be compliant.

V. LEGAL REQUIREMENTS

There are numerous laws that govern the protection and privacy of PII and there will only be more in the future. In the U.S., many of the laws are sector specific such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare entities or the Gramm Leach Bliley Act (GLBA) that is applicable to financial services companies, while others such as the State Security Breach laws apply to PII regardless of industry. Internationally, certain markets such as the European Union, Canada, Australia, Japan and Russia have stringent national data protection laws to protect the personal information of their citizens. This paper will not describe each of the privacy laws but instead will focus on a few of the key laws that pertain to hospitality companies to highlight the requirements and challenges.

A. THE FEDERAL TRADE COMMISSION'S POSITION

The FTC has a strong commitment to protecting the privacy of consumers that appears will only be stronger and more active in the future. The following excerpt from the FTC's website[4] summarizes the FTC's commitment.

> "Privacy is a central element of the FTC's consumer protection mission. In recent years, advances in computer technology have made it possible for detailed information about people to be compiled and shared more easily and cheaply than ever. That has produced many benefits for society as a whole and individual consumers. For example, it is easier for law enforcement to track down criminals, for banks to prevent fraud, and for consumers to learn about new products and services, allowing them to make better-informed purchasing decisions. At the same time, as personal information becomes more accessible, each of us - companies, associations, government agencies, and consumers - must take precautions to protect against the misuse of our information. The Federal Trade Commission is educating consumers and businesses about the importance of personal information privacy, including the security of personal information. Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information."

As it relates to privacy on the Internet and the controversial issue of behavioral targeting, in a March 10, 2009 speech by FTC Chairman Jon Liebowitz, he stated:

> "Internet privacy has been and will remain a foremost area of focus. On behavioral marketing, there are obviously benefits that targeting can bring to consumers in the form of more relevant advertising and the additional revenue that targeting can provide. This revenue may be vital to the survival of some industries. But we have to face the fact that the current model is not working. Staff recently issued guidelines identifying key components that a robust self-regulatory approach could be built around, and I'm hopeful that industry will respond with concrete improvements to the existing approach. Self-regulation, if it works, can be the fastest and best way to change the status quo. We will continue to monitor and report on developments and, if there isn't an appropriately vigorous response, my sense is that Congress and the Commission may move toward a more regulatory model. To be clear, we know our work in this area is not done or even near it. Online privacy is broader than behavioral targeting, and we will not neglect issues presented by data collection and its use for other purposes."

The FTC will be an active force in enforcing consumers' privacy in the future and shaping privacy practices.

[4] www.ftc.gov/privacy

1. FTC ENFORCEMENT ACTIONS

The FTC's commitment is not just in their words but is real as evidenced by their enforcement actions. The FTC has demonstrated the ability to successfully bring actions against companies that experienced data breaches under Section 5 of the FTC Act. The FTC has charged and entered into consent agreements with numerous companies under Section 5 of the FTC Act over the past several years for failing to adequately protect the personal information that was entrusted to them by their customers. In addition to monetary fines in some of the consent agreements, companies also agreed to independent biennial information security audits for a period as long as 20 years. The terms of these consent agreements are not attractive to any company but are a consequence of having a data breach that attracts the involvement of the FTC.

B. U.S. STATE SECURITY BREACH LAWS

In 2003, California enacted the Security Breach Information Act (SB-1386)[5] which requires companies that maintain certain PII about California residents to inform those individuals if the security of their information is compromised. This was the single most significant event in raising the stakes around information protection and privacy. Since 2003, forty-six other States, including the District of Columbia, have enacted similar laws. However, while these laws are similar, they are not identical. Specifically, there are differences in the definition of a breach, definitions of personally identifiable information, exceptions and notification requirements. Some of the State laws also require notification to the State Attorney General's office and/or Consumer Protection office. These laws have resulted in previously non-public events such as lost laptops containing PII now becoming public.

C. MASSACHUSETTS LAW

After several delays, on March 1, 2010 a new law in Massachusetts (201 CMR 17.00: Standards for the Protection of Personal Information of Resident of the Commonwealth)[6] goes into effect and will place unprecedented information security requirements on many companies that own, license, store or maintain PII concerning any Massachusetts resident. Unlike the current data breach laws, which are focused on actions that need to be taken after there is a data breach, this law includes numerous prescriptive proactive measures intended to protect PII from breaches. For many companies this law has a broad impact as it is not practical, and not wise, to segment PII based on residency of the individual and apply different security measures only to the data protected by this law. Some of the major requirements of this law require affected companies to:

- Maintain a written Information Security Program;
- Designate one or more employees to maintain the information security program;

[5] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
[6] http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

- Identify and assess internal and external risks to reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks;
- Provide on-going training;
- Implement policies with disciplinary action for non-compliance;
- Prevent terminated employees from accessing personal information;
- Require third party service providers to meet the security requirements and agree to the same in the contracts;
- Limit the collection, access to and storage of personal information;
- Maintain an incident response plan;
- Inventory all paper and electronic records and media that contain personal information;
- Regularly monitor and annually review security measures;
- Encrypt all personal information on laptops and portable devices; and
- Numerous specific computer security requirements.

Many companies will find it difficult to comply with all of the requirements of this new law as the reality of a challenging economic environment persists and resources tend to be dedicated to revenue generating and cost cutting activities. Nonetheless, companies will need to address these requirements or face the consequences, both in a court of law and the court of public opinion.

VI. RISK MANAGEMENT CHALLENGES

A. IT WON'T HAPPEN TO US

Denial or unwillingness by senior executives or others that are instrumental to gaining acceptance of the fact that a data breach can happen to your company can be the most difficult challenge to overcome. Some companies only learn through their own costly adverse experiences and fail to honestly assess and recognize risks until they materialize. It can be a sobering exercise to review the chronology of data breaches maintained by Privacy Rights Clearinghouse[7] and the nature of each breach. As you peruse the list, you will not find it difficult to envision your company being a victim of the same type of breach as one more of these other companies.

B. PROLIFERATION OF PII

A significant challenge in meeting business and legal requirements is that PII likely exists in many locations within and outside of your company. PII often exists in centralized systems, on laptops, Blackberrys, iphones, flash drives, CDs, at the homes of teleworkers, at third party service providers and at contractors of third party service providers. The presence of PII in those

[7] http://www.privacyrights.org/ar/ChronDataBreaches.htm

locations can greatly enhance employee productivity but also represents another location or "data store" that requires protection.

C. LIMITED RESOURCES

As previously stated, many companies simply do not have the required resources to conduct a thorough risk assessment and implement corrective actions where necessary. Adequate staffing by competent resources, whether they are employees or contractors, is a critical success factor to managing information protection and privacy risks. While committees can be helpful in setting direction and obtaining the necessary level of executive buy-in, committees generally are not effective at executing the level of detailed work necessary to manage information protection and privacy risks.

D. RESISTANCE TO CHANGE

Enhancing controls around the protection of PII typically requires business process and/or technology changes that may be resisted by employees. While it is somewhat natural and expected that changes may be resisted, it is important to be committed to the implementation of necessary changes. As an example, a relative simple change to enforce the use of passwords on Blackberrys will not go unnoticed and may result in comments about how this change is significantly adversely affecting productivity. Such reactions are typically exaggerated and subside a short time after the change is implemented. In addition, negative reactions can be lessened by proactively communicating all changes before they are implemented and explaining the business reasons and benefits of the change.

VII. GAUGING YOUR RISK

There are several questions you can ask to quickly gauge your company's information protection and privacy risks at a high level. The answers to these questions will rather quickly help you assess if appropriate and defensible actions have been taken. These high level questions include:

- Are adequate competent resources dedicated to this area?
- Is attention given to the necessary activities (e.g., policies, training, risk assessment and remediation, etc.)?
- Has a current risk assessment been performed?
- Is the risk assessment inclusive of all locations where PII is maintained?
- Are remediation plans prepared and implemented?
- Is senior management aware of the risks?
- Have insurance options been considered?
- Is residual risk documented and approved by senior management?
- Is there a process in place to manage risks and legal compliance requirements on an on-going basis?

If the answer to one or more of these questions is no, there is work to be done.

VIII. FUTURE OF PRIVACY LEGISLATION

The legal requirements around information protection and privacy will likely only become more stringent in the future, both in the U.S. and internationally. Several international markets already have stringent data protection laws and there are and have been an assortment of privacy related bills at the U.S. Federal level. In addition, individual States have shown that they will enact legislation that they believe is prudent to protect their residents.

A. ONLINE BEHAVORIAL ADVERTISING

In the U.S., there is significant discussion and debate regarding the need to regulate on-line behavioral advertising. This issue is also a topic of conversation outside of the U.S. On-line advertisers fear that regulation in this area would significantly stifle e-commerce by making it impractical for companies to deliver targeted advertisements and a personalized on-line shopping experience based on the consumer's past on-line behavior. Privacy advocates and some consumers are concerned that companies and the advertising service providers they engage are tracking their on-line activity and creating robust profiles of all of their on-line behavior that could be misused or used to the detriment of the individual. Considering the growing importance of e-commerce to overall economic growth, this topic will likely continue to be debated in the future and some level of regulation is more than a remote possibility.

B. U.S. NATIONAL PRIVACY LAW

Senator Leahy has authored S.1490 – Personal Data Privacy and Security Act of 2009[8] to:

- Prevent and mitigate identity theft;
- Ensure privacy;
- Provide notice of security breaches;
- Enhance criminal penalties;
- Enhance law enforcement assistance; and
- Enhance other protections against security breaches, fraudulent access, and misuse of personally identifiable information

At a high level, this bill if passed in its current form, would essentially nationalize the current State security breach laws and the new Massachusetts law (Standards for the Protection of Personal Information of Resident of the Commonwealth). Unlike financial services and health care companies that are already subject to information security legal requirements, passage of this bill would require hospitality companies to implement a myriad of proactive measures to

[8] http://www.thomas.gov/cgi-bin/query/C?c111:./temp/~c1110WHIgh

protect the security and privacy of PII. The financial consequences of non-compliance are also noteworthy with fines of $5,000 per day per violation, subject to a $500,000 maximum per violation that can double for an intentional or willful violation. While ultimate passage of this bill is unknown, it is likely only a matter of time before a national law is enacted.

C. INTERNATIONAL REGULATIONS

As previously stated, there are national data protection laws in markets such as the European Union, Canada, Australia, Japan and Russia. In addition, the Asia Pacific Economic Cooperation (APEC) privacy framework is gaining momentum and requires companies doing business in those markets to meet specific requirements related to the collection, processing, handling and transferring of PII. In the future there will only be more regulation in the international arena as well as refinements to existing data protection such as those currently underway to the Australia Privacy Act.

IX. RECOMMENDATIONS

There are several recommended actions your company should consider as you reflect on the state of your information protection and privacy efforts. The specific actions that will be most effective at your company depend on the current state of your information protection and privacy program and other dynamics in the organization.

A. PII MINIMIZATION

Protecting all PII in every location that it exists can be a very expensive strategy. The most impactful action you can take is also the most obvious – limit the amount of PII that needs to be protected. A core business practice should be to only collect the minimum amount of PII required to execute the business transaction, manage your workforce or meet any applicable legal requirement. The less PII that is collected and stored, the less that has to be protected and is at risk of breach. This can require simple or significant changes to current business processes and information systems but is worth the effort.

B. ELIMINATING DUPLICATE DATA

Duplicate PII is a common occurrence and can be identified by conducting a PII inventory. As an example, some golf clubs maintain a payment authorization form with the member's credit card details and also keep a photocopy of the credit card. Some hotels make an imprint of a guest's credit card even though it was swiped and authorized successfully. These practices are not only unnecessary, they create an extra paper record of the credit card that now must be protected and is subject to loss or theft. In addition, maintaining a photocopy of a credit card violates PCI DSS because the security code on the front or back of the card cannot be stored after transaction authorization.

Numerous instances of the same PII can also be found in computer systems, files on desktops or laptops, network servers, back-up tapes, portable media such as flash drives, CDs or back-up tapes and also in paper records. Each of these instances of PII must be protected and represents a data repository that can be lost or stolen.

The cost to protect duplicate PII can be substantial, not to mention the storage costs. Every reasonable effort should be made to minimize PII and the locations where it is stored to the minimum number of places practical to meet your business and legal needs.

C. SOCIAL SECURITY NUMBERS

Social security numbers deserve special attention because over time many companies have used the social security number as a static unique identifier for many purposes. The result is that this seemingly ideal unique identifier likely resides in numerous information systems and on paper forms. This information may pertain to job applicants, current employees, former employees, club members or others. While the social security number is needed for certain tax purposes, any use beyond that purpose should be discontinued and another means to assign a static unique identifier, not related in any way to the social security number, should be implemented.

D. INFORMATION DISPOSAL

After identifying duplicate information, it is important that the duplicate information that can be eliminated is securely deleted. For paper based records it is fairly straightforward as a cross cut shredder or third party shredding service can be used to securely destroy this data. For information stored on electronic media such as desktops, laptops, servers, flash drives, etc. it should be securely and permanently deleted. Technically, the information on these electronic devices could be restored with specialized software unless the disk space is overwritten or the device is destroyed. If the duplicate information that is to be deleted resides on electronic devices that are no longer needed such as old laptops, all information should be permanently deleted prior to disposal. In either case, if you do not have internal IT resources that have access to the specialized software to permanently delete all the information you should use a third party service provider that specializes in secure deletion of information from electronic devices. These service providers can also ensure any devices to be disposed of meets Environmental Protection Agency requirements.

E. SUCCESS IS A JOURNEY

Companies that successfully manage their information protection and privacy risks know that this is an on-going effort as risks and legal requirements change over time. Regardless of your current state, any tasks, no matter how modest, that can be completed to strengthen your company's position are worthwhile. It is not always practical to complete all tasks as quickly as desired but delaying all activities is not prudent. Instead, do as much as you can as resources permit.

F. BE PREPARED TO DEFEND YOUR COMPANY

If your company is the victim of a data breach or loss you need to take actions to defend and protect the company. All of the related business partners such as the credit card companies, merchant banks and third party service providers will not come to your rescue and perhaps may not even take responsibility for their issues that caused or contributed to the breach that are their accountability. Put simply, you will likely have no allies in the event of a breach.

X. CONCLUSION

Balancing customer expectations, business realities and managing legal compliance requirements in the area of information protection and privacy is a challenging task with significant consequences. While the task will only become more challenging in the future, like other business challenges, it is not insurmountable with the appropriate level of attention and understanding that to be successful it must be viewed as an on-going journey and not a destination. Just as there are winners and losers in sporting events where outcomes are most often determined by level of skill, information protection and privacy can also be viewed as a game where your success will be determined by the level of commitment and skill you invest.