PRINCIPLES OF PRIVACY
Defining & Implementing Sound Privacy Practices in Hospitality

Why is Privacy Important Today? ................................................................. 3
The Privacy Dilemma ............................................................................. 3
Threats to Privacy .................................................................................. 4
  Identity Theft Frauds ........................................................................... 4
  Credit Card Fraud ............................................................................. 5
  Violent Crimes or Theft ...................................................................... 5
  Data Use, Abuse or Discrimination .................................................... 5
  Undesired Marketing ......................................................................... 6
  Spam & Spam Filtering ...................................................................... 7
  Pornography ....................................................................................... 7
  On-Line Threats .................................................................................. 8
Privacy Regulation Around the World .................................................... 10
Commercial Self-Regulation ................................................................. 10
  The Payment Card Industry Data Security Standard ......................... 10
  Certification Seals ........................................................................... 11
  Direct Marketing Association ............................................................. 12
Privacy Regulation in the United States .................................................. 12
  CAN-SPAM ....................................................................................... 12
  Sarbanes-Oxley Act ......................................................................... 13
  Fair & Accurate Credit Transactions Act (FACTA) ............................ 13
  Industry-Specific Regulations .............................................................. 14
  California Notice of Security Breach Law ........................................... 14
  Possible Future Regulations ............................................................... 14
European Union Regulations ................................................................. 15
  European Union Privacy Directive 95/46/EC ....................................... 15
Safe Harbor ........................................................................................... 15
Safe Harbor Principles of Privacy .......................................................... 16
  Notice ............................................................................................... 16
  Choice .............................................................................................. 16
  Onward Transfer ............................................................................. 16
  Access .............................................................................................. 16
  Security ............................................................................................ 17
  Data Integrity .................................................................................... 17
  Enforcement ...................................................................................... 17
  Other Accepted Principles of Privacy ............................................... 18
Privacy Futures & Trends ...................................................................... 19
  Improved Spam Controls ................................................................. 19
  Biometrics ....................................................................................... 19
  Wireless ............................................................................................ 20
  Vehicle tracking ............................................................................... 20
  Location-Based Services ................................................................. 20
PRINCIPLES OF PRIVACY
Defining & Implementing Sound Privacy Practices in Hospitality

A prescriptive overview of the nature of practicing privacy in today’s hospitality industry. Written for the hotelier, the document presents enough of the technical, conceptual and legal framework surrounding privacy issues today to understand the actionable recommendations and to utilize the checklists.

Why is Privacy Important Today?

Hoteliers have been the trustees and guardians of guest privacy since the earliest inns. Guests maintain an explicit expectation of privacy as a core component of the guest-innkeeper relationship. Guest privacy’s central position in that relationship has been codified in both statutory and case law. Hotel guest privacy has been enshrined in this way for so long because hoteliers are privy to innumerable details about guest preferences and behavior. There is nothing new about the obligation of hoteliers and the expectation of guests.

What is new is the spotlight on privacy and data security in society at large, not just the hospitality industry. In recent months, major breaches of confidential personal information appear in the headlines weekly. Privacy issues are now high profile news stories, and no business wants to be the center of one of these stories.

Banking, financial and credit reporting companies have borne the brunt of bad publicity and litigation over privacy issues. That does not mean that the hospitality industry is not vulnerable to threats: rather it means only that money-oriented businesses are richer targets than hotels, but if a hotel company is not vigilant about collecting only data required and protecting that data, we will be reading about that company in the headlines as well.

Recognizing that the threat of bad publicity, litigation or fraud is a driver for adopting sound privacy practices, hotel companies must recognize that taking privacy seriously and doing it well is good business in a positive manner. Articulating and executing strong privacy policies in the hotel enterprise can only strengthen and reinforce the guest relationships that every hotel depends upon. A wise hotelier will make a commitment to guest and employee privacy and execute that commitment.

The Privacy Dilemma

Hotels, like many other businesses, capture and retain extensive information on their customers. At a minimum, this information is used to support business transactions, such as posting a pay-per-view movie transaction to a guest folio. The best hoteliers retain many of these details in some form solely for the purpose of improving guest service delivery in the future, such as recording a stated preference for a specific room or room type. Many guests both expect and appreciate the enhanced service levels made possible...
by capturing, retaining and using information about their past stays and preferences.

However, legitimate fears about the proliferation, capacity, long life and networking of computer databases that store a multitude of details about individuals has spawned a global privacy movement strongly opposed to capturing personally identifiable data. This movement has led to the adoption of varying laws governing data collection around the world and numerous industry-defined data privacy and security initiatives.

These two contradictory imperatives, collecting and using personal information about guests to improve service while not running afoul of the spirit or the letter of privacy regulations and laws combine to form what we term “The Privacy Dilemma”. By nature, hoteliers want to do whatever they can to improve service and repeat patronage, yet must do so in respect of the applicable laws.

Supporting AH&LA members in reconciling this dilemma drives the need for this booklet. The contents are intended to familiarize the hotelier with:

- The threats to privacy and their consequences
- The concepts behind applicable regulations
- Specific actions hoteliers we recommend hoteliers take relative to privacy

**Threats to Privacy**

The numerous actual and potential threats to privacy include both criminal and potentially discriminatory abuse. These threats are off-line as well as on-line. Most threats to consumer privacy revolve around either:

- Hackers, “dumpster divers” or “social engineers” steal customer data
- Employees steal data
- Companies lose or misplace data in storage or transit
- Corporations or government agencies misusing data

This section attempts to enumerate some of these threats in more detail.

**Identity Theft Frauds**

Identity theft (IDT) is generally considered the fastest-growing type of crime in North America. The Federal Trade Commission’s (FTC) Consumer Sentinel database tracked 246,570 complaints of identity theft frauds in calendar year 2004, a 52% increase over 2002*. Identity theft frauds can take various forms, but usually involve a fraudster getting credit in some manner (credit card, bank loan, even a mortgage) using the victim’s name and Social Security Number (SSN) and/or credit card numbers. Stealing credit card statements or promotions from the mail is one way this can be done.

* Note that the FTC treats all credit card fraud as a category of identity theft. Credit card fraud as a percentage of all IDT frauds has been declining, but increasing in absolute numbers.
Identity theft is a real problem for the victims: their credit history becomes compromised, they get hounded by creditors seeking collection for debts they never incurred and it costs them thousands of dollars and hundreds to hours to erase the frauds from their credit history. Law enforcement rarely treats identity theft investigations as a high priority compared to crimes of violence, so the risk to the fraudster is low.

Hotels typically have a low involvement in identity theft frauds as they do not normally offer credit cards themselves or collect Social Security Numbers. Hotels, like every other employer, have a specific obligation to protect confidential employee data such as SSNs. This protection includes limiting access to employment records, including systems that store SSN and other data. Access to these systems (Time & Attendance, Payroll and/or Human Resources Information Systems) should be tightly controlled and limited to those employees with a job requirement to access the data.

Credit Card Fraud

Typical credit card fraud simply entails fraudulently obtaining and using someone else’s card or card number. This differs from identity theft in that the fraudster does not attempt to obtain new credit in the victim’s name. Credit card frauds typically have a short life span, no longer than one billing cycle and are more likely to involve retail transactions than lodging transactions.

The hotelier’s privacy obligation relative to credit card frauds is to secure credit card numbers from theft. The most effective ways to do this are to “mask” or not display complete card numbers on folios, POS receipts, confirmations, screen displays or reports. Rather, show only a portion of the card number. Also destroy obsolete transaction records that may contain card numbers as required by the PC Data Security Standard (see below).

- Violent Crimes or Theft

A relatively rare threat to privacy includes crimes of violence enabled by a privacy transgression. An example here may include a hotel telephone operator inappropriately giving out a guest’s room number, which then allows the criminal to find the guest’s room and commit an offense. Obviously, a hotel has a high level of potential liability for any violence or crime perpetrated against a guest, more so if a failure or lack of hotel policy contributed to the crime in some way.

Data Use, Abuse or Discrimination

Many of the perceived threats to privacy revolve around the fear that someone could abuse private data to discriminate or otherwise act against a victim. People on the extreme of the privacy movement include police investigations as a threat to privacy and
not to be tolerated. We believe that most Americans do not agree with that position. Hotels should be prepared to release data to legitimate investigations supported by a subpoena. Many privacy policies state that the business will comply with any subpoenas and will notify the customer of any such request and compliance. A difficult gray area is how does one respond to a direct request for information by an officer in circumstances where there is no time to get a subpoena and delay could put someone at risk or a crime could be committed on hotel premises.

There are other very real threats to privacy in this category that the hotel is obligated to protect guests from. Folio detail should only include enough information to identify the transaction, for example, but not enough to show a specific telephone number called, for example. Hotels must ensure that requests for copies of folios are legitimate and are in fact from the guest herself rather than say, her husband’s divorce attorney. The process for confirming folio copy requests should be clear, documented and adhered to.

The general rule-of-thumb must be “It is no one else’s business what the guest did in the hotel so the hotel must protect that information from accidental or by-deception exposure.”

**Undesired Marketing**

Undesired marketing is perhaps the most common form of privacy abuse individuals experience at large. Today’s marketers can buy mailing and other lists based on any number of criteria (age, income, presence of children in the household, automobile ownership and more). These lists can then be used to market to the people on the list, who may or may not wish to be marketed to. This undesired marketing comes via direct mail, telephone or email.

With the proliferation of email utilization and email marketing, “spam” email has become a major nuisance to individuals and a substantial cost to companies. Because the marginal cost to the spammer of sending one more email message is zero, spammers have no incentive to target their lists to people that are likely to buy, but rather to get the largest possible number of addresses of any sort to broadcast to. Hence the ridiculous number of email messages blasted around the Internet hoping for a .0001% response rate.

The obligation of hotels in this regard is to not allow their guest lists to get out of the hotel company and to not engage in undesired marketing themselves, on-line or off-line. Most frequency program registrations include options to opt-in or opt-out of receiving messages from business partners and a separate opt-in decision for receiving messages from the frequency program.

The gold standard for email opt-in practices is the “double opt-in”, where an individual chooses or “opts-in” to receive marketing communications, which then automatically generates a confirming message to the provided email address. The message contains a link back to the host system which the consumer must click on to confirm that the
recipient was in fact the original registrant and does wish to receive communications. Less stringent practices include:

- **Single Opt-In** – Where an individual registers to receive communications but there is no verification that the registrant is the recipient.

- **Opt-Out** – Where an individual will receive communications until such time as they say they do not want to. Many consumers consider opting-out a risk for receiving more spam, fearing that the marketer now has validated that the address belongs to a real person.

The abuse of email marketing has given rise to much regulation and proposed legislation which we will discuss in more detail below.

**Spam & Spam Filtering**

A great deal of spam content sells pornography, erectile dysfunction drugs or makes other sexually-related offers. All employers, including hotels, have an obligation to provide a workplace free of sexually-charged influences. Most organizations prudently interpret this obligation to include keeping offensive email out of their corporate systems. Although not strictly a privacy issue, this very real concern is not too distant from privacy either.

Spam and preventing it are costly problems for businesses. The sheer volume of spam drives up required network capacity, a significant cost. Network administrators monitoring spam are expensive and the tools (primarily software filters) are costly. However, the potential of settling a sexual harassment suit makes these costs look minimal.

We strongly recommend that hotels and hotel companies use spam filters and other techniques to limit the amount of spam that comes into their network.

**Pornography**

Viewing pornography (on-line or otherwise) in the workplace introduces issues with both privacy and sexual harassment implications. Our position is that there is no place for this content in the workplace and that as employers we will act to interdict offensive inbound emails and employees are obligated to not introduce pornography or other potentially-offensive materials into the workplace. Many organizations enforce this policy with tools that restrict access to some sites, accepting the cost of employees not being able legitimate sites for business reasons that the tools misinterpret.

The privacy issue is whether or not the employer has the rights to be aware of what web sites and emails employees view and send. The current case law finds that if the computer and Internet access are property of the employer and the employee has signed an Acceptable Use Policy statement acknowledging this, then employees may be
disciplined for violations of the policy.

We recommend that hotels of any size require employees to sign an Acceptable Use Policy waiving privacy expectations, forbidding intentional viewing of pornography and forbidding downloading applications that could harbor spyware (see below).

**On-Line Threats**

**Phishing**

Phishing is the name given to the identity-theft technique of sending out emails that appear to be from a large, well-known company, typically a bank or other financial institution. The email tells the recipient that they must update their account information immediately and that they should click on a link in the email to do so. The legitimate-appearing link will take them to a web site constructed to resemble the requesting company’s and requests account numbers, user names, SSN, credit card numbers or other confidential details. The web site then captures the information and the fraudster can then attempt to transfer funds, apply for new credit and so on. A variation on the theme includes invitations to apply for loans or credit cards with attractive terms, tempting the victim to provide their SSN and other details.

Most phish attempts are relatively easy to identify, but the most effective approach is to simply never follow links from emails.

The exposure of hotel companies to phishing scams is minor. Having said that, hotel frequency programs should employ the same practice financial institutions use regarding address or email address changes: whenever an address is changed, send a letter or email to the previous address stating that the address of record has been changed and if this is in error, please contact the firm.

**Spyware**

Spyware is the generic name given to a broad class of offensive software that ends up on computers. This software can monitor keystrokes and report them to a remote server, replace your home page with one designated by the spyware, make pop-ups advertising things related to your searches appear or other offensive acts. Computers that become severely infected with spyware may be rendered unusable and are definitely security threats in the workplace as well as privacy threats to customers.

A spyware variation called *pharming* watches for the user of the compromised computer to point their browser towards a bank or other financial institution website. Then the spyware covertly re-directs it to a dummy site constructed to resemble the real one. The dummy site captures the attempt to log on (storing the username and password) and the perpetrators can then take over the account.
Spyware typically ends up a computer when downloaded by a user. “Free” programs that contain things people want (dancing smiley face icons, weather monitoring programs, many variations) typically require that the user accept a long, densely-worded Terms of Use agreement which no one bothers to read. The agreement gives the spyware manufacturer the right to add other software to the user’s computer, the spyware. Note that many of the aggressively-promoted “anti-spyware” products are in fact spyware themselves.

Removing spyware is a lengthy and boring process, typically requiring multiple anti-spyware programs (some anti-virus programs also have an anti-spyware component). It often does not completely eradicate the spyware, requiring a complete re-format of the hard drive on the machine, an even lengthier and more boring process.

The best solution to spyware is prevention: train users to not download applications from the Internet. Incorporate a prohibition on unauthorized downloading of software from the Internet into your Acceptable Use Policy. Purchasing licenses for legitimate anti-spyware applications is a very wise investment. Spyware comes in so many forms that no single anti-spyware application is likely to eradicate everything, leading many users to utilize more than one anti-spyware tool.
Privacy Regulation Around the World

The global privacy movement has inspired numerous efforts to regulate the collection and use of personally-identifiable data. Some of these efforts have been governmental. Others have been led by various industry associations, typically to forestall regulation by eliminating the need for it. While extremist privacy advocates typically decry self-regulation as a bad idea first and an utter failure second, we would consider the PCI Data Security Standard (often referred to as Visa CISP; see below) initiative a major victory for consumer privacy protection. Other meaningful “wins” for the consumer driven by the private sector include the various security and privacy certification services available that exist to give web site privacy policies a “seal of approval.”

Key observations about privacy regulation include:

- Expect more regulation in the future, not less

- In a global, networked economy the most stringent regulations in any substantial market will tend to become the de facto standard over time. A global hotel company based in the US with properties in Europe will, of necessity, take great pains to not violate privacy regulations in Europe, which typically means that customer data gathered in hotels in other jurisdictions will be accorded the same high standard of privacy.

Below, we discuss the various key regulatory initiatives currently in effect and proposed.

**Commercial Self-Regulation**

**The Payment Card Industry Data Security Standard**

American Express, Diners Club, Discover Card, JCB, MasterCard and Visa have come together to define a minimum uniform set of regulations for data security for all participants in the payment industry. This collaboration is specifically intended to protect consumer privacy, reduce fraud and increase trust in the entire payment processing value chain. The issuers call these regulations the Payment Card Industry (PCI) Data Security Standard. Many refer to it in shorthand as CISP, Visa’s acronym for Customer Information Security Program.

Highlights of the PCI Data Security Standard include:

Requires all issuers, merchants and systems to comply on a sliding timetable by size, with all but the smallest merchants in compliance by June 30, 2005

- Requires self-reporting of compliance
• Compliance enforced by offering proven-compliant merchants protection from fraud, with vastly greater exposure for non-compliant merchants

• Puts the burden of system vendor compliance on the merchant

• The hotel is responsible for ensuring that their credit card acquirer, PMS vendor, CRS vendor and others comply with the PCI Data Security Standard

• Requires establishment and documentation of stringent physical and logical access control and system administration practices, as well as regular testing of these practices

• Includes minimum standards for firewalls, wireless, anti-virus and more

• Some of the key system and business process requirements for compliance:
  
  o Do not store the full contents of any card track
  o Do not store the validation codes that are printed (rather than embossed) on cards
  o Store minimal account detail: name, account number and expiration date
  o Destroy all media with obsolete transaction data (like the night audit reports with thousands of credit card numbers on them in binders in the Accounting office)
  o Restrict access to complete card numbers on a need-to-know basis
  o Most system displays, reports and receipts may not show any more that the first six and last four digits of any card number
    ▪ Displaying the last four digits only is the most common implementation
  o Change all vendor default passwords before installing the system.
    ▪ Many hotels are in violation of this requirement

The key things for hoteliers to understand about this standard include:

• Compliance is not optional: if there is a fraud and the hotel or its systems are not in compliance, then the hotel is liable

• Most of the compliance points are pure common sense and/or good system administration practices

For more information on the PCI Data Security Standard, visit:  ?????
Another group of commercial self-regulation privacy initiatives of interest include non-profit organizations that have established privacy standards. They offer certification seals against their criteria and allow the organization to display the certification logo or seal.

Well-known privacy certifiers include:

- TRUSTe
- The Better Business Bureau
- WebTrust
- Entertainment Software Ratings Board (not relevant to hotels, but well-known as ESRB for games)

The purposes of the certifications are simply to inspire the consumer to trust that sites displaying the certification have proven that they are good stewards of consumers’ personal data.

**Direct Marketing Association**

The Direct Marketing Association (DMA) is a trade association of firms that operate by contacting consumers directly, be it traditional mail, telephone or email. The DMA has interests in promoting self-regulation as a means of forestalling governmental regulation.

**Privacy Regulation in the United States**

Compared to the European Union, privacy issues are lightly-regulated in the United States. In recent months, breaches and losses of privacy data, often massive, keep coming to light. Interestingly, the primary reason that these breaches are becoming known is due to a state regulation in CA-SB1386, discussed below.

The federal laws with the broadest application surrounding privacy include CAN-SPAM, Sarbanes-Oxley and the Fair & Accurate Credit Transaction Act (FACTA). *(Do we need to discuss Patriot Act??)*

**CAN-SPAM**

The CAN-SPAM Act intends to deal specifically with abusive email marketing. It includes penalties for transgression and adherence to the following minimum standards:

- Senders must have a prior and on-going business relationship with recipients. This might include registering to receive promotions on a website, booking a room on-line or being a hotel guest
- The subject line must accurately reflect the actual message content
• Sender firms must be clearly and accurately identified
• Sender’s full name and street address must appear in the message
• Sender must allow recipient to “Unsubscribe” by replying to or linking from the message

Although the flood of junk email continues, high-profile spammers are now being successfully identified, targeted and prosecuted. Perhaps these actions will reduce the abuse of email. In the meantime, all legitimate marketers, including hotels, will do well to adhere to the spirit and the letter of CAN-SPAM.

**Sarbanes-Oxley Act**

The Sarbanes-Oxley Act intends to compel higher levels of corporate governance and financial reporting integrity. One tactic employed in the bill requires public auditor certification that the systems and business processes in place provide an adequate level of internal control, security and data integrity. Auditing these practices will in fact drive the protection of consumer data as well as corporate integrity.

No public accounting firm would certify the statements of a hotel company that was not PCI Data Security Standard compliant.

**Fair & Accurate Credit Transactions Act (FACTA)**

FACTA, now taking effect nationwide*, allows consumers to request a free annual credit report from each of the three major credit reporting bureaus. Most experts consider regular review of consumer credit reports an important step in early detection of identity theft. FACTA contains numerous other provisions intended to assist victims of identity theft and those who believe their credit history contains errors. Like the PCI Data Security Standard, FACTA requires truncation of credit/debit card numbers and extends truncation protection to Social Security Numbers in copies of files. One FACTA provision requires the FTC to establish guidelines defining “Red Flag” indicators of possible identity theft and for banks to apply the Red Flags proactively. Another requires businesses to give consumers an opt-out for marketing communications from affiliates.

Some privacy advocates criticize FACTA for too many loopholes, too-long timelines for adoption and for limiting the ability of states to enact stronger laws. FACTA’s impact on hotels will be the legal requirements to secure stored data and destroy obsolete data in addition to the affiliate marketing opt-out clause. These clauses give legal teeth to the regulations already imposed by the PCI.

---

* Several key FACTA provisions are taking effect in phases, geographically, from West to East, with full effect September 1, 2005
Industry-Specific Regulations

The Gramm-Leach Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) both deal with privacy issues targeting specific industries. Gramm-Leach requires financial services firms to tell customers what data they gather and how they use it, and to have policies in place to prevent fraudulent or inappropriate access to it. HIPAA targets the health-care industry and intends to control disclosure of individual’s medical information.

The Benefits function of most employers, including hotels, have numerous obligations under HIPAA.

The Fair Credit Reporting Act (FCRA) of 1996 regulates the credit reporting industry. It embodies many of the principles discussed below under Safe Harbor.

California Notice of Security Breach Law

Effective July 1, 2003, the State of California adopted SB 1386, Notice of Security Breach Law. If any organization has gathered personal data of any California resident and then learns that the data has been accessed or lost in an unencrypted form, the organization is required to advise the resident of the breach.

This law is notable for several reasons:

- Many of the current wholesale privacy breaches we are now becoming aware of come to light only because of SB 1386, thus proving the concept that the strictest regulation becomes the de facto standard

- A federal version of the same law is under consideration, thus proving the concept that California often serves as a leading indicator for key trends in the rest of the nation

Another California law, SB27 “Shine The Light”, requires organizations that give customer information to third parties to tell any customers that ask about.

Possible Future Regulations

As noted above, a federal version of California’s Notice of Security Breach Law is under consideration, with stricter penalties for offenders.

Periodically, the issue of requiring encrypted storage of sensitive data is discussed as potential federal legislation. The Enterprise Strategy Group estimates that only 35% of financial firms encrypt data today.

The Schumer-Nelson Identity Theft Bill proposes to regulate firms that collect and sell
personal information with specific rules on preventing inappropriate access to such data.

**European Union Regulations**

**European Union Privacy Directive 95/46/EC**

Effective in 1998, the EU Privacy Directive (also known as the EU Data Protection Directive) demands that organizations implement deep and broad privacy protections. Data must be gathered only for legitimate business purposes and certain particularly sensitive data elements (ethnicity, political & religious beliefs, sexual orientation, etc) may not be collected. The directive also requires EU states to establish governmental authorities tasked overseeing data privacy policy implementation within their jurisdictions.

A key aspect of the Directive (Article 25) is that it prohibits the transfer of personally identifiable data to countries that do not offer the same protections of data as the Directive assures EU residents. Interpreted strictly, that means personally identifiable information about an EU resident may not be transmitted to hotel company CRS or web server in the United States, for example. This clause creates a clear business problem for US-based hotel companies and hotels, as well as other business. In fact, hotel companies and airlines have been the target of a number of EU-based investigations for violations.

In order to assure that the EU Directive does not become a barrier to international commerce, the EU and US Department of Commerce negotiated and adopted the “Safe Harbor” framework, essentially a set of rules that are deemed adequate to allow the transfer of such identifiable data with a minimum of administrative costs.

**Safe Harbor**

Adopted in 2000, the Safe Harbor framework allows US-based organizations to certify themselves as Safe Harbor-compliant. Such organizations may apply for listing with the EU as a compliant organization on a public website (http://export.gov/safeharbor). An important attribute of the Safe Harbor agreement requires most claims against US organizations to be heard in US courts rather than EU courts, provided that the organizations have a dispute resolution and compliance verification process in place. Failure to comply can result in Federal Trade Commission intervention with stringent civil penalties a possibility for fraudulent certifications.

The Safe Harbor framework rests upon seven core principles of privacy that have become generally accepted worldwide as sound privacy practices.

* Interestingly, very few of even the major US hotel companies have chosen to certify compliance under Safe Harbor, thus exposing themselves to litigation from any EU citizen
Safe Harbor Principles of Privacy

Below, we provide a brief summary of each of the Safe Harbor principles, along with a description of some of the implications of the principle for hotels and hotel companies.

Notice

Organizations must notify individuals what data they gather and for what business purposes. Notice must include a statement of how individuals may dispute or complain about data gathering and use. Organizations must also disclose any third parties to which information is disclosed (such as an outsourced Central Reservations service provider or a mailing house) and the means by which a consumer may limit the disclosure and use of such information.

Hotel privacy statements should be published on websites and include all the above elements of Notice. Hotel employees should be made aware of the Privacy statement including Notice.

Choice

Organizations must give individuals the choice to opt-out of third-party disclosures or any other disclosure other than the original purpose stated under the Notice principle. Sensitive information (health-related, for example) requires an explicit “opt-in” for any disclosure or alternate use.

Opt-out provisions should be clearly stated in all marketing communications to individuals. Hotels should generally require opt-in or double opt-in for email subscriptions.

Onward Transfer

The Notice and Choice principles must be applied in order to transfer data to an agent or other third party. The transferring organization is responsible for ensuring that the receiving third party complies with the Safe Harbor principles. Alternatively, the third party must agree in writing to adhere to the same level of data protection embodied in Safe Harbor. This principle, like Safe Harbor itself, transcends borders.

Hotels should verify that third parties they transfer data to comply with Safe Harbor principles.

Access

Under Safe Harbor, individuals have the right to review any personal information stored by the compliant organization. Individuals may correct amend or delete any personal information that is inaccurate. Safe Harbor permits exceptions where the cost of providing access is out of proportion to the risk of individual privacy, or the privacy
rights of other individuals may be affected by such access.

Hotels should provide this access subject to the proportional reasonableness test. For most hotels, including an invitation to contact the hotel to review and update information in the Privacy Statement should suffice.

**Security**

Organizations must take reasonable precautions against misuse, loss and unauthorized access or disclosure.

Implications of this principle for hotels include:

- Securing back up tapes and reports
  - Encryption of back up files is a good idea, but carries the risk of losing or forgetting the key built into an automated backup job
- Limiting access on a need-to-know basis
- Verifying caller identity before releasing data about hotel guests

**Data Integrity**

Compliant organizations must ensure that data gathered is relevant to the stated purposes of use. This includes ensuring that data gathered is accurate, complete and current for the intended purpose.

For hotels, this means gather only data you will use to serve the guest or market to them. Destroy obsolete data.

**Enforcement**

Enforcing compliance with the Safe Harbor principles entails two distinct areas:

- A clear and stated process of recourse for individuals who feel their privacy has been violated as defined by Safe Harbor
  - This recourse may ultimately result in legal action and the award of damages
- Procedures for verification of compliance with Safe Harbor
  - Persistent compliance violations may result in removal from the Safe Harbor roster, thus exposing the organization to legal action under the EU Privacy Directive
Other Accepted Principles of Privacy

The above principles are of central importance to US-based hotel companies that wish host guests from the European Union. Privacy advocates often identify other principles that may be implied by the seven Safe Harbor principles described above. Some of these include:

- Relevance – Data collected must be relevant to the stated purpose for which it is gathered. This principle is implied in the definition of the Safe Harbor principle of Data Integrity.

- Retention – Data must not be retained for longer than necessary under a reasonable retention policy, as implied in the Data Integrity definition.
Privacy Futures & Trends

As technology advances and commerce becomes more and more global in nature, many new influences will come into play that both benefit and threaten privacy. Below we discuss some of the more visible current and future technologies and trends that will affect privacy.

**Improved Spam Controls**

Spam is such a nuisance to individuals and businesses due to several key attributes

- The marginal cost of sending one more email message is zero, therefore the economics encourage spammers to send millions of emails to make tens of sales
- Email and the Internet are global by nature and identifying the location or enforcing regulation on a spammer in a remote part of the world is difficult
- Email technology, including routing and the construction of message headers, is well-understood by spammers and subject to abuse

Hope is on the horizon for new technologies that will address one or more of these attributes. Some are focused on the zero marginal cost attribute, and intend to change that by imposing a “tax” on sending an email. This “tax” would take the form of computing power rather than money, with no impact on legitimate individual correspondents but imposing significant computer processor overhead on mass-mailings. Other approaches are focused on improving the authentication of email sources. The Sender ID Framework (SIDF) and Sender Policy Framework (SPF) are two approaches using IP-based technologies. DomainKeys (Yahoo!) and Identified Internet Mail (Cisco) are signature-based authentication techniques.

**Biometrics**

Like many privacy-related technologies, biometrics (the science of using finger or palm prints, retina scans, DNA, facial features, voice prints and other features of one’s body to identify an individual) represent both an opportunity and a threat: another dilemma. Biometrics can protect one’s privacy by ensuring that only an authorized user can gain access to information or a location. However, for biometrics to work, the data defining the metric (palm print, for example) must be stored somewhere, raising the possibility of abuse.

Biometric technology for access control and identification is still in its infancy. The most common adoption today is in biometric time clocks. These clocks are effective in preventing others from punching an employee in or out. Their installation has been
challenged on privacy grounds in some businesses, but adoption continues.

**Wireless**

The proliferation of wireless communications technologies has numerous privacy implications. As with biometrics, these technologies offer both benefits and threats. Below we discuss some of the near-term futures.

**Vehicle tracking**

The best-known vehicle tracking technology is the On-Star service marketed by General Motors. Using a combination of cellular and Global Positioning Service (GPS) technology, On-Star operators can identify the precise location of subscriber vehicles at any time. The service enables giving voice directions if the driver gets lost and can automatically notify the operators in case of an accident. This ability is central to the On-Star value proposition of safety on the road. Yet, it presents a privacy threat if an operator or the service were to abuse the knowledge of a subscriber’s location.

The Lo-Jack vehicle tracking service also identifies precise locations, but only when activated by police when a vehicle is reported stolen.

There have been proposals made to equip all vehicles with GPS transmitters in a “black box” to enable authorities to track vehicle locations at all times. We believe that no such service will ever be implemented in Europe or North America based on privacy concerns.

**Location-Based Services**

Location-based Services (LBS) use either GPS or triangulation techniques to advertise the location of a cellular telephone. Benefits include enabling 911 emergency responses and the ability to find something near the user. Visualize asking your cell phone to “find the nearest hotel” while on the highway: since the phone advertises your location, an LBS database can return the name, distance and directions to the nearest hotel and even initiate a call to check availability. Other marketing opportunities proposed include the ability to send a virtual coupon to a cell phone when it approaches a business, perhaps offering a discount on rooms, food, umbrellas on a rainy day, etc.

All new cell phones in the US are equipped with some form of LBS for 911 purposes. Some advertise location for other location-based services, with the option to turn the LBS advertisement off.

**Radio Frequency Identification (RFID)**
Radio-Frequency Identification (RFID) describes the capability of placing small, inexpensive radio transmitters into objects, shipping containers, clothing, pets or people. The transmitters broadcast a unique serial number to a nearby receiver, which then logs the location and timestamp in a database. The best-known current RFID implementation is Wal-Mart’s requirement that their large vendors implement RFID tagging on shipping pallets to further enhance their already formidable supply chain management capabilities. Other current RFID implementations include casino chips (pit bosses can know precisely how much people wager, no estimating) and subcutaneous insertion of transmitters into pets.

RFID applications generate countless privacy concerns. As applications come to market, more concerns will accompany them. While applications like tracking shipping containers are benign, extending the capability to actual retail items and linking them to the individuals who purchase them may not be.

Some hotel RFID applications to watch for include:

- **Asset tracking** - placing RFID tags on things like uniforms that move around and are subject to loss
- **Employee Monitoring** – giving security or other mobile personnel RFID tags that allow management to confirm that they are making their rounds or to identify the nearest employee to handle a guest service request

### Wi-Fi Abuse

Wireless data networking, usually abbreviated as Wi-Fi, enables organizations to set up data networks without wires, allowing untethered visitors and employees access to the public Internet or private networks. Like all forms of Internet communications, Wi-Fi communications are inherently not secure. Unencrypted Wi-Fi transmissions can be readily intercepted. The basic encryption in many Wi-Fi access points is known to be “hackable.” Improving technology is reducing the threat of a hacker intercepting someone else’s data packets, but the risk remains. This is a clear privacy and commercial risk.

Many if not most hotels in North America offer some form of Wi-Fi service to guests. Hotels should have a strong Terms of Use statement on their Wi-Fi service that explicitly removes any expectation of privacy and places the burden of security and encryption on the user. The entry screen should be constructed in such a way that users must accept the Terms of Use before continuing to use the service.

Many hotels use their Wi-Fi networks for administrative applications. These might include remote check-in services, front door guest recognition or allowing sales managers to check rates and dates while visiting with a client in the lobby lounge. Hotels should
always utilize a Virtual Private Network (VPN) on the wireless devices to protect guest or administrative data from interception.

Wi-Fi abuse is a tangible risk area for hotels.

**Password Vaults/Services**

The proliferation of on-line services that people utilize on a daily basis means a proliferation of usernames and passwords. In order to help people manage their ever-increasing number of accounts, a number of services and tools have come into the market to make it easy to either store usernames and passwords or to log onto the service (i.e., Microsoft Passport) which then logs you on to other services you have subscribed to. Some variations include financial websites that sweep your account data from other financial sites to present a consolidated view of your entire financial life (consumer banking, mortgage, brokerage, 401(k), etc).

Another privacy dilemma, while it may be convenient to store accounts, usernames and passwords in a central location, if that location is compromised, the subscriber’s entire financial life is at risk.

Password vaults are not a meaningful risk area for hotel companies.

**Trusted Traveler Program**

Following 9/11, airport security became much more rigorous and intrusive. Some observers attribute the hassles, monotony and long lines with discouraging travel. The Transportation Security Administration has a pilot program in place allowing individuals to apply for “trusted traveler” status which allows them to replace much of the airport screening process with a retinal scan.

This program has the benefit of reducing some airport-related headaches, but some privacy advocates see giving up a retinal scan as a privacy violation.

**National Identity Cards**

Every so often, a cry for a national identity card arises in Washington, DC. Predictably, this cry immediately gets shouted down by the privacy lobby. The arguments for a national identity card include:

- A single, consistent national format will be less susceptible to forgery than 50 different drivers license formats
- A national identity database could facilitate criminal or other inquiries by authorities
• Issuance can be tied to legal immigration status, and expire with visas, thus reducing perceived threats from illegal aliens

Privacy advocates cite the same arguments against national identity cards.

**Employee Monitoring**

Many organizations, especially in contact centers, monitor employee’s use of computers and telephone systems. Monitoring may take the form of recording conversations and keystrokes. The business purposes of such monitoring include quality assurance, productivity measurement and creating a record of a transaction (when a customer requests a stock transaction by telephone, for example).

Other forms of employee monitoring include scanning employee data files, email and instant messages, web sites visited and so on in addition to video surveillance.

Some consider monitoring a privacy intrusion. Another way to look at it is an employee protection against an unjust complaint by a caller or a defense against some other alleged misdeed.
Checklists

Hotel(s)
Website(s)
Contact Centers
Policy Elements

Hotel Operations Policy Elements

- At registration, write down room number assignments and hand to guests across the Front Desk, do not speak the number aloud

- Many experts advise requiring a photo ID issued by a government agency in order to register. Some hotels photocopy the ID, which then puts a burden on the hotel to secure and destroy the copy

- Enforce strict policies against giving out room numbers over the telephone or front desk

- Giving new or duplicate keys only to registered guests that can show ID

- Minimize the use of guest names and room numbers in radio or telephone conversations

- Do not show guest names on reports given out for newspaper drops

- Do not allow third parties to do amenity drops, bag pulls or other activities on guest room floors

- Train room attendants to keep room assignment sheets in their pockets rather than on their carts, especially if names appear on the report

- Ensure that Expected Departure folios delivered to guest rooms the night before checkout are slid completely underneath doors all the way into the guest room and cannot be pulled back into the corridor

Privacy Policy Elements

Employee Appropriate Use Policy Elements
More Information

Government Sites

Business & Industry Sites

Privacy Advocacy Organization Sites