prism.
travel & leisure consulting.

Articles / Whitepapers

Practice: Technology

Topic: Privacy & Security

The Privacy Dilemma

Hotel guests explicitly expect that innkeepers will respect and protect their privacy as part of the guest-innkeeper relationship…

By Mark G. Haley, CHTP

There is nothing new about this expectation: it is a longstanding and central obligation to the guest, and has been for centuries, codified in statutory and case law.

What is new about privacy that creates a dilemma for the hotelier?

- The spotlight on privacy issues in society at large, due in part to the proliferation of computer networks and databases storing personal information
- The equally-strong expectation on the part of guests, particularly in upscale and luxury segments, that hoteliers will capture and retain key profile data in order to improve service delivery in future visits

Let us evaluate each of these two "horns of the dilemma" in more detail.

Spotlight on Privacy

For many years now, a global privacy movement has been generating momentum. Consumer fears of abusive or inappropriate use of personally identifiable information have driven the privacy movement worldwide. The concern is that marketers, for good or ill, will attempt to profit from using consumer data for any purpose other than which it was provided in the first place. In the hotel environment, these purposes typically include:

- To satisfy legal requirements, such as registering for a hotel room
- To support a transaction, such as paying for a hotel bill
- To ensure that specific needs or wants are met during the stay, such as a non-smoking room or a dietary requirement

The global privacy movement has led to a literal smorgasbord or regulations and law around the world. Until recently, the best-known and widely-enforced privacy regulation has been the European Union Privacy Directive 95/46/EC[1], generally referred to simply as the EU Privacy Directive, is a principles-based approach to privacy protection and regulation that affects . The Directive applies to all

[1] For a deeper understanding of privacy regulation in general, the EU Privacy Directive and Safe Harbor, please see the AH&LA publication "Principles of Privacy" by Mark G. Haley, CHTP and Jungson Kim, ©2009, American Hotel & Lodging Association

EU residents, irrespective of where the data is maintained. Thus, a hotel loyalty program based in the United States with members residing in the EU must adhere to the Privacy Directive. This adherence is generally met by following the Safe Harbor framework, which outlines the same principles for US-based companies with European customers.

More recently, the Payment Card Industry Data Security Standards[2] (PCI DSS or simply PCI), enforced by the credit card industry, takes aim at privacy in terms of the protection of credit card information more so than all personally identifiable information. Rather than being principle-based like the EU Privacy Directive, the PCI DSS defines much more specifically the steps required to protect cardholder data, both in on-line and off-line environments. The ownership and maintenance of the PCI DSS rests with a non-profit organization called the PCI Security Standards Council, with enforcement of the standards reserved to the issuing credit card brands (Visa, American Express, MasterCard, Discover and JCB). The brands enforce compliance with fines imposed on the merchant's credit card acquirer, who then passes the fines onto the merchant.

Other relevant regulations include FACTA, CAN-SPAM, Sarbanes-Oxley, various Notice of Security Breach Laws and more.

The things to understand about privacy regulation:

- Expect more regulation and more-stringent regulation in the future
- The strictest regulations tend to become de facto standards, rather than a higher bar in some other jurisdiction

Guest Expectations of Higher Service Levels

The other horn of the dilemma is with expectation that a hotel company will recognize the guests that have stayed with them before, and will deliver service levels based on preferences and other information the guest has provided before. This could be as simple as retrieving an address or remembering a non-smoking room type request, to providing a specific welcome amenity based on a profile submitted through the hotel company's loyalty program. Other expectations revolve around making it easier to interact with the hotel company on-line, by retaining details from the guest's profile, enabling the easy look-up of past folio detail or future reservations, guest-maintenance of profile data and more.

Industry leaders such as Ritz-Carlton, Denihan and Fairmont have succeeded with these flavors of customer-friendly services. The win is to truly demonstrate to the guest that the hotel company "knows" them and welcomes them back as guests of the brand, even if it is the first visit to that particular property. And given the success of these companies, the evidence shows that guests respond to this higher level of service and become advocates for the brand rather than merely customers.

EU Privacy Directive & Safe Harbor Principles

Notice – Hotels must notify the guest what information is gathered and why

Choice – Guest must have the choice to opt-out of any disclosure. Sensitive information requires opt-in

Onward Transfer – If information is transferred to another party, the Notice and Choice principles must apply

Access – Guest must be able to review and correct profile information at any time

Security – Hotels must take reasonable precautions against loss, misuse or unauthorized disclosure of guest data

Data Integrity – Hotels must ensure that data gathered is relevant to the stated purpose

Enforcement - Guests must have a clear path of recourse should they feel their data has been misused; Hotel company must have a method for verifying compliance

[2] For more on PCI for hotels, please see the AH&LA publication "The PCI Compliance Planning Process for Lodging Establishments", by Mark G. Haley, CHTP and Daniel J. Connolly, PhD, © 2008, American Hotel & Lodging Association

For an upscale or luxury hotel company to compete with the rest of the market in these segments, the hotel company must find their own means of delivering these "high-touch" services, all of which depend on the capture and re-use of articulated and observed guest preferences.

Reconciling the Dilemma

So, these two powerful forces appear to create a dilemma for the hotel company:

How to deliver the enhanced services demanded by the guests to win their loyalty, while ensuring that guest information is never miss-used or subject to loss in any manner?

In my experience, the path to reconciling the dilemma starts with the hotel employees and ends with the strict regulatory compliance practices:

- Establish a culture of privacy in the hotel company
    - Have someone designated as clearly in charge of information privacy, with the commensurate skills, title and budget
    - Task this individual with establishing and promulgating a clear and intelligible information privacy policy that is both consistent with the Safe Harbor principles and enhanced service delivery
    - Examine all aspects of privacy, including off-line: folio copy requests, giving out room numbers, etc; not just information stored in databases
- Make it clear to customers why you are collecting certain information (i.e., to improve services or to support necessary transactions)
    - Never utilize or allow a third-party to utilize that information for any other purpose

Pursue and maintain PCI compliance and consider extending the encryption and other relevant requirements to the entire guest profile as well as the credit card data. ■

Mark G. Haley, CHTP, is a partner with The Prism Partnership LLC, a Boston-based consultancy servicing the global hospitality industry. For more information, please visit: http://theprismpartnership.com or call 978-521-3600.

Article first published in: Hospitality Upgrade