THE
NATIONAL LAW REVIEW

Hotels, Hospitality and Guest Privacy: Six Important Questions to Ask After Andrews Verdict

Thursday, March 17, 2016

Earlier this month, a *Nashville* jury awarded sportscaster ***Erin Andrews*** $55 million after she sued the companies that franchise, own and operate a hotel, alleging that the hotel improperly gave her private information to another guest, who then invaded her privacy. The following is a list of questions that savvy hoteliers should be asking in order to help protect themselves in the wake of the *Andrews* verdict.

Article By Tanya L. Curtis
Claudia Callaway Terry Green
Christina E. Hassan
Katten Muchin Rosenman LLP Advisories

Litigation / Trial Practice
Communications, Media & Internet
Labor & Employment
Tennessee

1. Do We Have Policies and Procedures in Place That Reflect Our Commitment to Guest Privacy?

The first question for any owner or manager is whether a comprehensive set of policies and procedures are in place that accurately reflect your company's commitment to the privacy of its hotel, restaurant and spa guests. Do these policies and procedures comply with applicable state and federal law? Is the management group bound by any property owner policies and procedures? Is a state or federal privacy disclosure required in the spa or salon?

2. Do We Have a Mechanism to Track Employee Privacy Training?

During the *Andrews* action, some hotel employees testified that they could not recall the property's privacy policies. Does your company have a robust training and tracking system for its policies and procedures? Has your company developed periodic testing on such policies? Does the operative franchise or property management agreement require such training and/or testing?

3. What Do Our Property Management Contracts Say About Liability and Indemnification?

In the *Andrews* action, the court dismissed the franchisor prior to trial based upon its lack of action related to Ms. Andrews's claims. What do your company's management and/or franchise agreements say about similar actions—and responsibility for the outcomes arising from the same?

4. Do We Have Appropriate Safeguards in Place to Prevent Unauthorized Access to Internal House Phones and Computers?

In the *Andrews* matter, the defendant testified at deposition that he learned of Ms. Andrews's room number by accessing a phone at the hotel restaurant's hostess stand that had an LCD screen that displayed the room number of guest to whom a call was made—he dialed the operator, asked to be connected to Ms. Andrews, and captured the room number that appeared on the LCD screen. Could this type of unauthorized access happen at your property? In addition to password protecting computer terminals and requiring a key to access point of sale terminals, consider requiring a personal code for calls made from "publicly" located internal phones.

5. Is Our Data Encrypted?

In many cases, *commercially reasonable* encryption can be the difference between a "data incident" and a data breach disaster. For example, many states have provisions in their data incident notification laws that exempt a company from notifying consumers regarding a data breach where the company encrypted the subject data.

6. Do We Have Insurance Coverage for Data Incidents?

Data incidents come in many different forms, ranging from an anonymous system hack from outside of the country, to the installation of point-of-sale "skimmers" that capture credit card data, to unauthorized, "on-property" access of guest information. Does your company have coverage for any or all of these incidents? To whom does that coverage apply and what are its limits?

Source URL: https://www.natlawreview.com/article/hotels-hospitality-and-guest-privacy-six-important-questions-to-ask-after-andrews