

presented by insights

# Hewlett Packard Scandal Highlights Investigative Reporting Privacy Issues

By P. Blake Keating, Vice President, Claims — First Media

*media·insights is published periodically by OneBeacon Professional Partners to address the broad scope of exposures faced by our agents' and brokers' clients, as media-related companies are scrambling to meet the public's appetite for information, news and entertainment in an increasingly litigious society. This issue of media·insights looks at invasion of privacy, identity theft and fraud arising from illegal or simply unsavory newsgathering techniques and recommends practical solutions for mitigating these costly exposures.*

Business leaders and the media can learn important lessons from Hewlett-Packard's ill-conceived plan to uncover leaks between corporate board members and reporters.

The resignation by former chairman Patricia Dunn revealed a lengthy corporate internal investigation replete with spying on journalists, the creation of fake employees and e-mailing of computer spy ware, all in an effort to uncover a confidential source and “plug” leaks from within HP. An article on CNET.com, which contained information that was released through an “unapproved” corporate channel, triggered the investigation by HP. Not only did this flawed plan damage the company's credibility within its ranks, but invited scrutiny – and criticism – from public officials and the world at large, as well as criminal charges and recent inquiries from the Securities and Exchange Commission.

The California Attorney General criminally charged Ms. Dunn and Kevin Hunsaker, Chief of Ethics officer, as well as three outside investigators, on four California state privacy felony charges: (1) fraudulently obtaining private information from a public utility; (2) accessing computer data without permission; (3) identity theft; and (4) conspiracy to commit the foregoing crimes.

The HP plan included the creation of a fictitious, unhappy executive who would plant stories and trick a journalist into revealing his or her confidential source(s) within the company. The plot was complicated, far-reaching and relied in significant part upon technology. For example, personal phone records were obtained under false pretenses, and spy ware, which is a software program that covertly gathers user information through the user's Internet connection without his or her knowledge, was sent to a reporter by e-mail. There have also been allegations in respect to hidden surveillance of board members, their families and a reporter.

While ostensibly victims in this case, journalists often draw fire of their own for going too close to “the line” of illegal, unethical or perhaps “just plain unsavory” newsgathering methods. In such instances, the media is well advised to slow down and ask a few preliminary questions: Is there any person or organization that might object to the methodology being contemplated or the revelation of the results of same? Is

there exposure to legal liability? Have the methods to gather the information been fully disclosed to a supervisor or even newsroom counsel? What if the newsgathering methods were disclosed during a trial? Are the reporter's own ethics or standards called into question? Reservations as to any of these questions may well indicate the presence of a potentially questionable practice. The preceding list is, of course, not exhaustive. Newsgathering practices should be discussed in advance with the editorial staff, as well as outside counsel. In the final analysis, the means of getting the information must justify the ends.

Journalists should be aware that the utilization of false pretenses to obtain a story is strongly disfavored, even if no law has been broken. A well-known example is the *Food Lion* case wherein reporters went undercover to investigate meat counter practices and expose unsanitary conditions at Food Lion supermarkets. While post-trial relief was granted by a federal appeals court, a jury found ABC's PrimeTime news show liable for \$5.5 million in punitive damages at the trial level. The litigation was time consuming and very expensive.

Certain newsgathering actions are unlawful, such as obtaining telephone records without the phone customer's consent, which is illegal under both state and federal law. Additionally, violation of laws such as the Computer Fraud and Abuse Act and wire fraud and identity theft statutes may also have occurred in the Hewlett-Packard case,

---

among others. Individuals do not want their privacy violated in a brick and mortar environment nor on the Internet, and laws are being drafted to protect such rights.

Because the exposure is significant for claims arising from newsgathering, media companies that disseminate news and information must make sure that they have adequate insurance in place that will provide broad coverage for privacy perils, including intrusion upon seclusion and public disclosure of private facts. Moreover, a claim for invasion of privacy can arise without an actual broadcast or publication. It is important that coverage apply for newsgathering activities even if there has not been an actual utterance or dissemination of media content. The newsgathering act, in and of itself, should be enough to trigger coverage.

© 2006 First Media, a division of OneBeacon Professional Partners  
The contents may be reproduced by recipients provided proper attribution is given. Material is provided for general informational and illustrative purposes and is not to be considered legal or risk management advice. Readers should consult their counsel for legal advice concerning publicity and privacy rights.



**OneBeacon**<sup>SM</sup>  
PROFESSIONAL PARTNERS

OneBeacon Professional Partners  
30 Tower Lane Avon, CT 06001  
tel 860.773.6150  
[www.onebeaconpro.com](http://www.onebeaconpro.com)