

What Lawyers Need to Know about Pretexting

IN 2005, PATRICIA DUNN, the chairman of the board of directors of Hewlett-Packard, ordered an investigation into leaks to various news reporters from someone on the board regarding confidential company information. An information broker obtained some of the board members' telephone records and was able to ascertain who on the board had made calls to news reporters. In 1999, a woman intent on discovering her fiance's worth hired an information broker to discover his checking account balance. The information broker obtained the amount for the fiance. Also in 1999, Liam Youens paid an Internet research company, Docusearch, to find out Amy Boyer's work address. The company discovered her home address, phone number, and Social Security number—but not her work address. Docusearch hired an information broker, who subsequently obtained and supplied the address. Youens drove to Boyer's workplace and fatally shot her as she left work.

Each case involved an information broker who obtained personal information by pretexting—pretending to be someone else. “Pretexting” has been defined by the Federal Trade Commission as “the practice of getting personal information under false pretenses,” with “personal information” being bank and credit card account numbers, information in a credit report, bank account and investment portfolio information, and Social Security numbers. Pretexting was specifically outlawed in 1999 under the Gramm-Leach-Bliley Act, which also made it illegal to solicit others to obtain financial information via pretext.

The woman who inquired about her fiance's bank account was—unknown to the information broker—actually an FTC investigator. After the broker supplied her with the information, the FTC filed suit to halt the operations of the broker's company (and two other information broker companies). The brokers were accused of using false pretenses, fraudulent statements, or impersonation to illegally obtain consumers' confidential financial information. The FTC and the brokers settled the matter when the brokers forfeited money they made while using pretexting. Also, they were prohibited from engaging in any activity in connection with obtaining, offering for sale, or selling personal financial information obtained by:

- Misrepresenting their identities or their right to receive customer information.
- Using others to obtain information using deception.
- Selling or disclosing customer information obtained from a financial institution.
- Making false and misleading statements.

In the *Docusearch* case, the information broker obtained Boyer's work address by placing a call to Boyer and then lying about her identity and the purpose of her call to convince Boyer to reveal her work address.¹ A subsequent police investigation revealed that Youens

maintained a Web site containing references to stalking and killing Boyer. The court said, “We conclude that an investigator who obtains a person's work address by means of pretextual phone calling, and then sells the information, may be liable for damages under [New Hampshire] Revised Statutes Annotated Chapter 358-A to the person deceived.”

In the HP case, Dunn hired a private investigation firm to find out the source of the leak. She instructed the private investigation firm to use legal techniques. The private investigation firm hired a third party who used pretexting to obtain phone records from the telephone

A federal bill, the Data Accountability and Trust Act, would prohibit an information broker from obtaining or disclosing any personal information or any other information relating to any person by making a false, fictitious, or fraudulent statement.

company, according to the SEC filing. These records show the phone number of the recipient of the call and the day, time, and duration of the call. The broker probably obtained these records the same way Locatecell.com did. Until it was shut down by the Missouri attorney general in January 2006, for \$110 Locatecell provided a list of the outgoing calls from a subject's phone from the last billing cycle. All that was required was the subject's name, address, and phone number. One could place an online order and get results within hours. Law enforcement surmises that Locatecell obtained records either from telephone company employees who were violating their companies' rules and simply selling customers' phone call records to information brokers and investigators or that information brokers and investigators were using pretexting (pretending to be the customer) to obtain records from the phone companies. Both Verizon and Cingular Wireless have sued companies who have sold their customers' cell phone records to third parties.

Neither the HP case nor the Boyer case involved obtaining financial records. In fact, HP's outside counsel, according to the SEC filing, advised HP that the use of pretexting at the time of the investigation was not generally unlawful, except with respect to financial institutions. On the other hand, according to a July 8, 2005, *Washington Post* article, Joel Winston, associate director of the

Carole Levitt and Mark Rosch are principals of Internet For Lawyers and coauthors of *The Lawyer's Guide to Fact Finding on the Internet*.

FORENSIC CONSTRUCTION DEFECT & ENGINEERING, INC.

A PROFESSIONAL CORPORATION

Forensic Analysis &
Investigation of:

- Construction Defects
- Structural, Civil, Environmental, Industrial Engineering & Issues for All Types of Structures and Buildings
- Regulatory Compliances & Building Codes



This Corporation can also provide expert witness in the areas of Malpractice Litigation or Real Estate transactions.

MASSIE MUNROE, M.S., P.E.
PRESIDENT & CEO • EXPERT WITNESS

Tel: 213-632-1310
Fax: 213-632-5299

E-mail: massie@ConstructionDefect.us
www.ConstructionDefect.us

VISUAL FORENSICS®



“EVIDENCE YOU CAN SEE™”

- Computer Animations start at \$2,500
- Any accident, scene, or object from any viewpoint
- In-house scientific, engineering and graphics expertise
- Medical illustrations

As seen on 60 Minutes, ABC, CNN, NBC

Free consultation & demo call:
800-426-6872 or 925-837-2083
www.visualforensics.com

VISION SCIENCES RESEARCH CORP.

VISION PERCEPTION
VISIBILITY AND HUMAN FACTORS

Arthur P. Ginsburg, Ph.D.

Expert Witness for:

Vision-Related Auto, Air, Locomotive
Pedestrian, And Work Accidents
Opposing Demonstrative Evidence Analysis
Site Visibility Analysis
Vision-Related Medical Malpractice
(*RK, PRK, Lasik – 20/20 not enough*)
800-426-6872 or 925-837-2083
www.contrastsensitivity.net

Morris Polich & Purdy LLP

Is Pleased to Announce
the Following New Partners & Associates

Partners

Gary A. Hamblet Insurance Coverage & Litigation
Stephen H. Huchting Insurance Coverage

Associates

Insurance Coverage	Harry A. Enfijian
Construction & Design	Ben J. Galante
Healthcare	Sue Junn
Products	Diana Kotler
Products/Environmental Commercial Law Construction & Design	Kristina M. Pfeifer
Civil Litigation	Raina L. Roessler
Products/Environmental	Richard E. Stultz
Products	Zachary J. Wadle
Construction & Design	Brian K. Walters



www.mpplaw.com

LAS VEGAS

LOS ANGELES

SAN DIEGO

FTC's Financial Practices Division, said: "The FTC views pretexting as a deceptive practice even without a specific ban on its use for telephone records." At any rate, pretexting to obtain telephone records no longer falls within a gray area. The Telephone Records and Privacy Protection Act of 2006 made it a federal crime for data brokers or others (except police) to pretext to obtain telephone records.

Other bills may expand the definition of pretexting. California Senate Bill 328 has private investigators and information brokers concerned about their ability to use pretexting to obtain almost any personal information about a person. The bill would "prohibit any person...from...obtaining or attempting to obtain, or causing or attempting to cause the disclosure of, personal information about a customer or employee contained in the records of a business through specified methods, such as by making false, fictitious, or fraudulent statements or representations." A federal bill, the Data Accountability and Trust Act, would prohibit an information broker from obtaining or disclosing any personal information or any other information relating to any person by making a false, fictitious, or fraudulent statement.

Despite recent cases involving pretexting, new federal laws making it illegal to pretext to obtain phone records, and various proposed federal and state laws expanding pretexting to a broad range of information, 42 percent of organizations surveyed by Deloitte Financial Advisory Services in 2007 admitted that they do not have written guidelines against the use of pretexting. Another 42 percent did not know if they had guidelines or stated it was not applicable to their business. Eight percent have guidelines and are satisfied with them, while another 5 percent have guidelines but are no longer satisfied with them.²

Under Rule 3-110 of the Rules of Professional Conduct, lawyers have a "duty to supervise the work of subordinate attorney and non-attorney employees or agents." In this time of antipretexing laws, lawyers should consider having written guidelines instructing their subordinates and agents to avoid pretexting—at least for phone records and financial information. Lawyers might also want to track proposed bills that are intended to broaden antipretexing laws beyond financial information and telephone records, such as California Senate Bill 328 and federal bill H.R. 958. ■

¹ *Remsburg v. Docusearch*, 816 A. 2d 1001 (N.H. 2003).

² See http://www.deloitte.com/dtt/press_release/0,1014,sid%253D2281%2526cid%253D141472,00.html.