

# BB REVIEW

## Intellectual Property Newsletter

### PRETEXTING

## INVESTIGATION BY DECEPTION WHERE ARE THE LIMITS?

By Will Hill Tankersley and Conrad Anderson IV

#### What's Inside . . .

##### Page 1

What is "Pretexting?"

Existing Laws

##### Page 2

Specific Uses for Pretexting

##### Page 3

Considerations in  
Pretextual Practices

##### Page 4

Conclusion

**For Further Information on  
the Intellectual Property  
Practice Group,  
Please Contact . . .**

#### **Birmingham, Alabama**

Will Hill Tankersley  
205-226-3424  
[wtankers@balch.com](mailto:wtankers@balch.com)

#### **Montgomery, Alabama**

Dorman Walker  
334-269-3138  
[dwalker@balch.com](mailto:dwalker@balch.com)

#### **Atlanta, Georgia**

Matthew B. Ames  
404-962-3561  
[mames@balch.com](mailto:mames@balch.com)

#### **Jackson, Mississippi**

R. Pepper Crutcher  
601-965-8158  
[pcrutcher@balch.com](mailto:pcrutcher@balch.com)

#### **Gulfport, Mississippi**

R. Mark Alexander  
228-214-0417  
[malexander@balch.com](mailto:malexander@balch.com)

### What Is "Pretexting"?

Pretexting is a simple investigative tool: An investigator approaches a target and, under the "pretext" of being someone else, obtains information that the target would ordinarily provide to such a person. It is this combination of a disguised identity and freely given information that makes pretexting a valuable, but potentially risky, technique.

The information acquired through such practices, if admissible in court, could have a dramatic effect on the outcome. Pretexting has a powerful confessional element with unguarded (and presumably truthful) responses by an investigative target. Information generated through pretexting may be more readily obtained in comparison to traditional discovery methods. Indeed, use of such a technique could reveal that the target is behaving lawfully, thereby avoiding a conflict. Such "deceptive" investigative methods do, however, raise legal and ethical questions. Moreover, the response by judges and juries to pretexting would need to be carefully considered.

### Existing Laws

In 2006, officials of Hewlett-Packard used pretexting to get the phone records of the company's directors so that they could determine who was calling the press and giving inside information. The practice worked and the leak was discovered, but the company's directors and the public at large were not impressed with the covert technique. As a result, the CEO and legal counsel resigned or were fired. The surreptitious tactics also prompted Congress to pass the Telephone Records and Privacy Protection Act of 2006

("TRPPA"). The TRPPA prohibits obtaining confidential phone records through the use of false or fraudulent statements, representations, or documents. It also prohibits purchasing or receiving the records from another, preventing attempts at outsourcing, or willful ignorance. Penalties include fines of up to \$250,000 and up to 10 years in prison.

Prior to the passage of the TRPPA, the Federal Trade Commission used its powers to halt the operations of several online data brokers pedaling consumer phone records. The FTC Act prohibits "unfair practices," defined as those that are likely to cause consumers substantial injury not reasonably avoidable and not outweighed by benefits to consumers or competition, and gives the Commission authority to seek injunctive and other equitable relief in federal district courts. In May 2006, the FTC filed five lawsuits alleging that the defendants in each case violated the Act by obtaining and selling consumer telephone records without consent. The FTC learned of the activities through the defendants' websites advertising their ability to obtain confidential customer phone records. The FTC settled three of the cases and won the other two, with the courts in each entering permanent injunctions barring the defendants from selling consumer phone records and personal information and requiring disgorgement of the profits from their activities. The FTC is currently litigating a sixth suit filed in February 2007.

In early 2007, the FTC was also behind an effort to pass the "Prevention of Fraudulent Access to Phone Records Act," a bill very similar to the TRPPA but which would allow the FTC to recover civil penalties from violators – currently, injunctions and disgorgement are the only remedies available under the Act. The bill did not make it out of committee.

### Visit Our Offices . . .

1901 Sixth Avenue North  
Suite 2600  
Birmingham, Alabama 35203

1710 Sixth Avenue North  
Birmingham, Alabama 35203

2 Dexter Avenue  
Montgomery, Alabama 36104

30 Ivan Allen, Jr. Blvd., NW  
Suite 700  
Atlanta, Georgia 30308

1310 Twenty-Fifth Avenue  
Gulfport, Mississippi 39501

401 East Capital Street  
Suite 200  
Jackson, Mississippi 39201

1275 Pennsylvania Avenue,  
N.W.  
Washington, D.C. 20004

### Visit Our Website:

[www.balch.com](http://www.balch.com)

If you no longer wish to receive this update or have an address change, please contact:

Nora Yardley  
205-226-3476  
[nyardley@balch.com](mailto:nyardley@balch.com)

### Disclaimer and Copyright Information . . .

*This publication is intended to provide general information. It is not intended as a solicitation, and in the event legal services are sought, no representation is made that the quality of legal services to be performed is greater than the quality of legal services performed by other lawyers. The listing of any area of practice does not indicate any certification of expertise in the area as listed. ©2007. Balch & Bingham LLP. All rights reserved.*

While the TRPPA clearly protects consumers' telephone records, it does nothing more. However, there are other laws in place relating to the ability to gather or disclose other personal information. For example, the Gramm-Leach-Bliley Act ("GLBA") is now the centerpiece for financial privacy. The GLBA requires financial institutions to provide notice of their privacy practices to customers and give them the opportunity to choose how their personal financial information (PFI) is shared. Additionally, the GLBA has a "Safeguard Rule" which requires institutions to design, implement, and maintain procedures to protect customer information. The GLBA also contains a specific pretexting section which makes it a crime to obtain, or attempt to obtain, customer information from financial institutions through false, fictitious or fraudulent statements or representations. Penalties include fines of up to \$100,000 per violation for organizations, \$10,000 per violation for officers and directors, and up to 5 years in prison.

In addition to the GLBA, consumers find some financial privacy protection from the Fair Credit Reporting Act ("FCRA"). The FCRA allows a person to obtain a consumer's credit report where the person has a "legitimate business need" either in connection with a business transaction initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account. Several courts have examined whether a party to litigation has a "legitimate business need" for obtaining an adverse party's credit report and generally find such a need only where the litigation concerns the collection activity on an account.

In a case specifically concerning pretexting, the Superior Court of Massachusetts held that a group of defendants violated the FCRA when they impersonated consumers to obtain their credit reports and subsequently sold their personal financial information. *Commonwealth v. Source One Assocs.*, 10 Mass. L. Rep. 579 (Mass. Super. Ct. 1999). Such violations of the FCRA can carry severe criminal and civil consequences. The statute provides for fines and/or imprisonment for up to two years for "[a]ny person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses." A person who obtains a consumer report under false pretenses is also liable to the consumer reporting agency for the greater of \$1,000 or actual damages. For willful noncompliance with the FCRA, a person will further be liable to the individual consumer for actual loss and possibly even punitive damages. All of these provisions permit recovery of court costs and attorneys fees.

Businesses and individuals who use consumer reports for business purposes are also subject to the "Disposal Rule" which requires implementation of measures to dispose of consumer information to prevent unauthorized access or use. The Disposal Rule does not have strict requirements applicable to every organization, but rather is flexible and allows for an individualized determination of reasonable measures based on the sensitivity of information, the costs and benefits of various disposal methods, and changes in technology.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") does not specifically address pretexting. However, HIPAA requires "covered entities" to safeguard private health information (PHI). A pretexter attempting to gather HIPAA-protected information may nevertheless, be subject to liability under other tort theories such as trespass, fraud and the like.

### Specific Uses for Pretexting

Notwithstanding the dangers of pretexting for telephone records, PFI, or PHI, pretexting has been permitted in Intellectual Property ("IP") investigations. For example, manufacturers have been allowed, within limits, to determine whether a retailer is infringing on or diluting the manufacturer's trademark. An investigator simply goes into a store and, under the pretext of being an ordinary consumer, engages in a transaction. Courts tend to allow such practices in the IP context because this kind of activity would be difficult to otherwise detect and because "confidential" or private information is not being sought. Courts generally require that such investigations be undertaken in the same manner that the general public would encounter the alleged wrongdoer. In other words, courts do not tolerate attempts to "trick" anyone into doing or saying things that they ordinarily would not, but will permit undercover investigation and observation of the suspect's routine and ordinary practices. Indeed, Alabama's Center for Professional Responsibility has specifically held that, within limits, a lawyer may employ a private investigator to engage in such activity in the context of an IP investigation.

The practice of pretextual calling has also been permitted to detect unlawful discrimination. In one case, investigators were sent to Shell gas stations, under the pretext of being customers, to test whether Shell employees were requiring black patrons to pre-pay while allowing white customers to pay after they had pumped their gas. The court held that it was permissible to have investigators seek such services in the same manner as the general public, and it also was permissible to videotape such transactions. The court suggested, however, that certain



conduct would go too far, such as tricking employees into doing or saying things outside of the normal business routine, interviewing them, or asking them to fill out questionnaires. *Hill v. Shell Oil Co.*, 209 F. Supp. 2d 876 (D. Ill. 2002).

Courts have applied the same rationale to permit undercover investigation of housing and employment discrimination, where a “tester” poses as an interested tenant or prospective employee.

Finally, there are somewhat bizarre examples of pretexting. For example, three lawyers in Massachusetts allegedly set up fake job interviews with a Judge’s law clerk in an effort to investigate an alleged judicial conflict of interest. The Massachusetts State Judge was not amused and ordered the disbarment of two lawyers and the suspension of a third.

## Considerations in Pretextual Practices

Assuming that none of the previously mentioned laws are implicated, businesses or individuals may find pretexting to be a helpful investigative tool, particularly for suspected infringement of intellectual property rights. Clients and counsel should be aware, however, that the subject of the pretextual investigation will undoubtedly learn of the practice after a lawsuit is filed and will be very disturbed by the clandestine technique. Probing discovery and argument about the permissibility of the practice should be expected. The specific facts of the situation and

the investigation will dictate how the judge views the activity. Perhaps even more important, however, is how the jury will react to the “undercover” investigation. Even though the investigation could uncover wrongdoing, a jury might not be sympathetic to a pot calling the kettle black.

**Will Hill Tankersley** is a partner at Balch & Bingham LLP and leads its Intellectual Property (“IP”) litigation practice. He is the founder and was the first president of the Alabama State Bar Section on IP, has many IP clients (large and small) and he is a frequent speaker and writer on IP. He holds an LLM in Trade Regulation (IP and Antitrust) from NYU. He has been a Deputy Assistant Attorney General to assist the State of Alabama on IP disputes. He was a subcommittee chairman for Alabama’s version of the Uniform Electronic Transfer Act and is an arbitrator for WIPO. After college (W&L) and before law school (University of Alabama), he served in the Infantry and Special Forces. He can be reached at 205-226-3424 or by e-mail at wtankers@balch.com.

**Conrad Anderson IV** is an associate at the Birmingham, Alabama office of Balch & Bingham. He attended the University of Mississippi for both undergraduate and law school. Conrad’s practice includes advice and representation of various litigation matters for large corporations, small businesses and individuals. He can be reached at 205-226-3415 or by e-mail at canderson@balch.com.