

TABLE OF CONTENTS

I.	<u>CURRENT FEDERAL LAWS PROHIBITING PRETEXTING</u>	3
	Gramm-Leach Bliley Act of 1999, P.L. 106-102	
	Telephone Records and Privacy Protection Act of 2006, P.L. 109-476	
	Federal Trade Commission Act, Section 5	
II.	<u>PRETEXTING BILLS IN THE 110th CONGRESS</u>	8
	Data Accountability and Trust Act, H.R. 958	
	Consumer Telephone Records Protection Act of 2007, H.R. 852	
III.	<u>PAST CONGRESSIONAL HEARINGS REGARDING PRETEXTING</u>	11
	<u>Hearings Related to Phone Records (2006-2007)</u>	
	<ul style="list-style-type: none">• House Committee on Energy and Commerce – “<i>Phone Records For Sale: Why Aren’t Phone Records Safe from Pretexting?</i>” (February 1, 2006)• Senate Committee on Commerce, Science, and Transportation – “<i>Protecting Consumers’ Phone Records</i>” (February 8, 2006)• House Committee on Energy and Commerce – “<i>Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?</i>” (June 21, 2006)• House Committee on Energy and Commerce – “<i>Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?</i>” (June 22, 2006)• House Committee on Energy and Commerce – “<i>Hewlett-Packard’s Pretexting Scandal</i>” (September 28, 2006)• House Committee on Energy and Commerce – “<i>Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?</i>” (September 29, 2006)	

Hearings Related to Financial Information

- House Committee on Banking and Financial Services – “*Use of Deceptive Practices to Gain Access to Personal Financial Information*” (July 28, 1998)

IV. EXISTING AND PENDING STATE PRETEXTING LAWS 16

Section 638 of the California Penal Code (Senate Bill 202 of 2006)

Pending California Legislation – Senate Bill 328 (Bill Number: SB 328)

V. OVERVIEW AND ANALYSIS OF STATE & FEDERAL PRETEXTING CASE LAW & PROFESSIONAL ETHICS ISSUES RELATED TO THE USE OF PRETEXTING BY ATTORNEYS 18

Fishing With Dynamite: “How Lawyers Can Avoid Needless Problems From ‘Pretextual Calling’” (Alabama State Bar Magazine) 2008

Understanding Investigative Pretexts (www.beaprivateeye.com) 2002

The Truth Behind Pretexting: In-house Investigations and Professional Responsibility Concerns (Robbins, Kaplan, Miller and Ciresi, LLP) 2007

Electronic Privacy Information Center (EPIC): “Letter to Ethics Board Concerning Attorneys' Use of Pretexting” 2006

VI. POSITIONS OF THE PRIVATE INVESTIGATIONS COMMUNITY AND REGULATORS ON PRETEXTING 23

National Council of Investigation & Security Services (NCISS)

Federal Trade Commission (FTC)

International Association of Security and Investigative Regulators (IASIR)

State Licensing Requirements for Private Investigators

VII. PRESS REPORTS OF PRETEXTING SCANDALS 24

I. CURRENT FEDERAL LAWS PROHIBITING PRETEXTING

[Gramm-Leach Bliley Act of 1999, Public Law 106-102](#)

The Gramm-Leach-Bliley Act makes it illegal for anyone to:

- Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents.

Gramm-Leach-Bliley Act

[15 USC, Subchapter II, Sec. 6821-6827](#)

Fraudulent Access to Financial Information

Sec. 6821 – Privacy protection for customer information

- (a) Prohibition on obtaining customer information by false pretenses.
- (b) Prohibition on solicitation of a person to obtain customer information from financial institution under false pretenses.
- (c) Nonapplicability to law enforcement agencies.
- (d) Nonapplicability to financial institutions in certain cases.
- (e) Nonapplicability to insurance institutions for investigation of insurance fraud.
- (f) Nonapplicability to certain types of customer information of financial institutions.
- (g) Nonapplicability to collection of child support judgments.

Sec. 6824. Relation to State laws

(a) *In general*

This subchapter shall not be construed as superseding, altering, or affecting the statutes, regulations, orders, or interpretations in effect in any State, except to

the extent that such statutes, regulations, orders, or interpretations are inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.

(b) *Greater protection under State law*

For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 6822 of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

[Telephone Records and Privacy Protection Act of 2006, P.L. 109-476](#)

The Telephone Records and Privacy Protection Act of 2006 amends the federal criminal code to prohibit the obtaining, in interstate or foreign commerce, of confidential phone records information from a telecommunications carrier or IP-enabled voice service provider (covered entity) by: (1) making false or fraudulent statements to an employee of a covered entity or to a customer of a covered entity; (2) providing false or fraudulent documents to a covered entity; or (3) accessing customer accounts of a covered entity through the Internet or by fraudulent computer-related activities without prior authorization. Imposes a fine and/or imprisonment of up to 10 years.

Sec. 1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

(a) Criminal Violation- Whoever, in interstate or foreign commerce, knowingly and intentionally obtains, or attempts to obtain, confidential phone records information of a covered entity, by--

- (1) making false or fraudulent statements or representations to an employee of a covered entity;

- (2) making such false or fraudulent statements or representations to a customer of a covered entity;
- (3) providing a document to a covered entity knowing that such document is false or fraudulent; or
- (4) accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section 1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates

Federal Trade Commission Act, Section 5

The Federal Trade Commission Act (Section 5) bars "unfair or deceptive acts" in business practices, and according to the FTC, "generally prohibits pretexting for sensitive consumer information."

The following is an excerpt from Statement of the FTC at a July 1998 U.S. House Banking Committee Describing the use of the FTC Act to stop pretexting:

FTC Authority to Combat the Act of Pretexting to Obtain Confidential Information

Given the limitations of the IRSG Principles, the Commission will need to address the problem of pretexting by doing what it does best -- law enforcement. Indeed, although the Commission encourages industry self-regulation, the Commission is first and foremost a civil law enforcement agency, whose mandate is to combat unfair and deceptive practices. And the practice of obtaining confidential information for resale under false pretenses appears to be just that -- unfair and deceptive.

In cases of unfairness or deception, the Commission can issue administrative complaints, conduct administrative adjudications, and issue cease and desist orders.⁽²³⁾ Further, in cases of fraud and other serious misconduct, Section 13(b) of the FTCA authorizes the Commission to seek injunctive and other equitable relief in federal court.⁽²⁴⁾ In a Section 13(b) action, a court may exercise the full breadth of its equitable authority, including the issuance of a permanent injunction and "any ancillary relief necessary to accomplish complete justice."⁽²⁵⁾ This authority

includes the power to order consumer redress and to compel disgorgement of a defendant's ill-gotten gains.⁽²⁶⁾ The Commission has filed over 500 Section 13(b) cases in federal court.

We believe the act of pretexting by information brokers likely violates the FTCA's prohibition of "unfair or deceptive acts or practices in or affecting commerce" and would warrant filing a Section 13(b) action in federal court to obtain equitable relief.⁽²⁷⁾ First, making misrepresentations to a financial institution to obtain confidential information for resale may be a *deceptive* act affecting commerce.⁽²⁸⁾ Second, representing to customers that information will be obtained legally, when in fact it can be obtained only through actions that likely violate the FTCA and certain other statutes⁽²⁹⁾ may also be a *deceptive* act affecting commerce.⁽³⁰⁾

In addition, obtaining and reselling a consumer's confidential financial information may be *unfair* acts, in violation of Section 5. To establish an unfairness theory, the Commission must show (1) that the practice of obtaining consumers' private financial information without permission or under false pretenses causes, or is likely to cause, substantial injury; (2) that the injury is not outweighed by countervailing benefits to consumers or competition; and, (3) that consumers could not have avoided the injury.⁽³¹⁾

First, we believe that the invasion to consumers' privacy observed here may constitute substantial injury.⁽³²⁾ In some instances, the ability of a third party to use a consumer's financial information can cause substantial monetary harm. In assessing injury, a court may consider, among other things, whether the conduct violates public policy as established by "statute, common law, industry practice, or otherwise."⁽³³⁾ The value our society places on protecting the privacy of financial information is demonstrated by federal statutes that protect the confidentiality of individuals' financial information such as the Fair Credit Reporting Act,⁽³⁴⁾ the Right to Financial Privacy Act,⁽³⁵⁾ the Electronic Fund Transfer Act,⁽³⁶⁾ as well as numerous state statutes,⁽³⁷⁾ state court decisions holding that banks have an implied duty to maintain the confidentiality of financial information,⁽³⁸⁾ and the precautionary practices employed by the banking industry to protect their account holders' information.⁽³⁹⁾

Second, harmed consumers, because they typically have no way of knowing that an information broker was attempting to access their financial information, cannot avoid the

injury. Finally, using false pretenses to obtain confidential bank account information appears to provide no countervailing benefit to consumers or competition.⁽⁴⁰⁾

In short, we believe the Commission likely would succeed in a law enforcement action against pretexters, either on a deception or unfairness theory. We also believe that we could obtain significant remedial relief, including a permanent injunction against the practices, disgorgement of ill-gotten gains, and/or consumer redress.

[Link to Full Prepared Statement](#)

[Back to Table of Contents](#)

II. PRETEXTING LEGISLATION IN THE 110th CONGRESS

[Data Accountability and Trust Act, H.R. 958](#)

Sponsor: Rep. Bobby L. Rush (D – IL)

Date of Introduction: February 8, 2007

Status: Referred to House Subcommittee on Commerce, Trade and Consumer Protection

Language Regarding Pretexting:

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY

(c) Special Requirements for Information Brokers-

(5) PROHIBITION ON PRETEXTING BY INFORMATION BROKERS-

(A) PROHIBITION ON OBTAINING PERSONAL INFORMATION BY FALSE

PRETENSES- It shall be unlawful for an information broker to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, personal information or any other information relating to any person by--

- (i) making a false, fictitious, or fraudulent statement or representation to any person; or
- (ii) providing any document or other information to any person that the information broker knows or should know to be forged, counterfeit, lost, stolen, or fraudulently obtained, or to contain a false, fictitious, or fraudulent statement or representation.

(B) PROHIBITION ON SOLICITATION TO OBTAIN PERSONAL INFORMATION

UNDER FALSE PRETENSES- It shall be unlawful for an information broker to request a person to obtain personal information or any other information relating to any other person, if the information broker knew or should have known that the person to whom such a request is made will obtain or attempt to obtain such information in the manner described in subsection (a).

- (d) Exemption for Telecommunications Carrier, Cable Operator, Information Service, or Interactive Computer Service- Nothing in this section shall apply to any electronic communication by a third party stored by a telecommunications carrier, cable operator, or information service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153), or an interactive computer service, as such term is defined in section 230(f)(2) of such Act (47 U.S.C. 230(f)(2)).

Consumer Telephone Records Protection Act of 2007, H.R. 852

Sponsor: Rep. Jay Inslee (D – WA)

Date of Introduction: February 6, 2007

Status: Referred to House Subcommittee on Telecommunication and the Internet

Language Regarding Pretexting:

SEC. 2. FINDINGS.

Congress finds that--

(1) customer telephone records may be accessed without authorization of the customer by--

(A) an employee of the telephone company selling the data;

(B) 'pretexting', whereby a data broker or other person pretends to be the owner of the phone and convinces the telephone company's employees to release the data to them; or

(C) unauthorized access of accounts via the Internet; and

(2) because telephone companies encourage customers to manage their accounts online, many set up the online capability in advance. Many customers never access their Internet accounts, however. If someone seeking the information activates the account before the customer, he or she can gain unfettered access to the telephone records and call logs of that customer.

SEC. 3. UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN CONNECTION WITH OBTAINING CONFIDENTIAL PHONE RECORDS INFORMATION OF A COVERED ENTITY.

(a) Prohibition on Obtaining Confidential Phone Records Information Under False Pretenses- It shall be unlawful for any person in interstate or foreign commerce to knowingly and intentionally obtain, or attempt to obtain, confidential phone records information of a covered entity, by--

(1) making false or fraudulent statements or representations to an employee of a covered entity;

(2) making such false or fraudulent statements or representations to a customer of a covered entity;

(3) providing a document to a covered entity knowing that such document is false or fraudulent; or

(4) accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section 1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates.

[Back to Table of Contents](#)

III. PAST CONGRESSIONAL HEARINGS ON PRETEXTING

Hearings Related to Phone Records (2006-2007)

House Committee on Energy and Commerce – “*Phone Records For Sale: Why Aren’t Phone Records Safe from Pretexting?*” February 1, 2006

Witnesses:

Panel 1

Mr. Kevin J. Martin - *Chairman; Federal Communications Commission*

Mr. Jon Leibowitz - *Commissioner; Federal Trade Commission*

Panel 2

Ms. Lisa Madigan - *Attorney General, State of Illinois*

Mr. Steve Largent - *President and Chief Executive Officer; Cellular Telecommunications and Internet Association*

Mr. Edward Merlis - *Senior Vice President, Law & Policy; United State Telecom Association*

Mr. Marc Rotenberg - *Executive Director; Electronic Privacy Information Center*

Mr. Robert Douglas - *Chief Executive Officer; PrivacyToday.com*

[Link to the Statements and Testimonies](#)

Senate Committee on Commerce, Science, and Transportation – “*Protecting Consumers’ Phone Records*” February 8, 2006

Witnesses:

Panel 1

Mr. Charles E. Schumer - *United States Senator, New York*

Panel 2

Ms. Kris Monteith - *Chief of Enforcement Bureau; Federal Communications Commission*

Ms. Lydia Parnes - *Director; Bureau of Consumer Protection, Federal Trade Commission*

Mr. Marc Rotenberg - *President and Executive Director; Electronic Privacy Information Center*

Mr. Robert Douglas - *Chief Executive Office; PrivacyToday.com*

Ms. Cindy Southworth - *Director of Technology and Director of the Safety Net Project;*
National Network to End Domestic Violence

[Link to the Statements, Testimonies, and Transcript](#)

House Committee on Energy and Commerce – “*Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?*” June 21, 2006

Witnesses:

Panel 1

Mr. Adam Yuzuk – *Atlantic Beach, NY*

Panel 2

Mr. James Rapp - *Touch Tone Information*

Mr. David Gandal - *Shpondow.com*

Panel 3

Mr. John Strange - *Worldwide Investigations*

Ms. Laurie Misner - *Global Information Group*

Mr. Jay Patel - *Abika.com*

Mr. Tim Berndt - *Relia Trace Locate Services*

Mr. Ed Herzog - *Global Information Group*

Mr. James Welker - *Universal Communications Co.*

Mr. Skipp Porteous - *Sherlock Investigations*

Mr. Patrick Baird - *PDJ Services*

Ms. Michele Yontef - *TelcoSecrets.com*

Mr. Steven Schwartz - *First Source Information Specialists*

Mr. Carlos Anderson - *C.F. Anderson, PI*

[Link to the Statements and Testimonies](#)

House Committee on Energy and Commerce – “*Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?*” June 22, 2006

Witnesses:

Panel 1

Mr. Peter Lyskowski - *Assistant Attorney General; Missouri Attorney General’s Office*

Ms. Julia Harris - *Assistant Attorney General; Florida Attorney General's Office*

Panel 2

Mr. Paul Kilcoyne - *Deputy Assistant Director of Investigations; U.S. Immigration and Customs Enforcement*

Ms. Elaine Lammert - *Deputy General Counsel, Investigative Law Branch; Federal Bureau of Investigation*

Mr. James J. Bankston - *Chief Inspector, Investigative Services Division; U.S. Marshals Service*

Ms. Ava Cooper Davis - *Deputy Assistant Administrator, Office of Special Intelligence, Intelligence Division; U.S. Drug Enforcement Administration*

Mr. W. Larry Ford - *Assistant Director, Office of Public and Governmental Affairs; Bureau of Alcohol, Tobacco, Firearms, and Explosives*

Panel 3

Mr. Raul Ubieta - *Police Major, Miami-Dade Police Department; Economic Crimes Bureau*

Mr. David L. Carter - *Assistant Chief of Police; Austin Police Department*

[Link to the Statements and Testimonies](#)

House Committee on Energy and Commerce – *“Hewlett-Packard’s Pretexting Scandal”*

September 28, 2006

Witnesses:

Panel 1

Mr. Darren Brost - Austin, TX

Mr. Bryanh Wagner - Littleton, CO

Mr. Charles Kelly - Villa Rica, GA

Ms. Ann Baskins - *Senior Vice President, General Counsel and Secretary; Hewlett-Packard Company*

Mr. Ronald R. DeLia - *Managing Director; Security Outsourcing Solutions, Inc.*

Mr. Anthony Gentilucci - *Manager, Global Security Investigations; Hewlett-Packard Company*

Mr. Joe Depante - *Owner; Action Research Group*

Ms. Cassandra Selvage - *Eye in the Sky Investigations, Inc.*

Mr. Kevin T. Hunsaker - *Senior Counsel, Legal Department; Hewlett-Packard Company*

Ms. Valerie Preston - *In Search Of, Inc.*

Panel 2

Mr. Fred Adler - *IT Security Investigations; Hewlett-Packard Company*

Mr. Larry W Sonsini Esq. - *Chairman; Wilson Sonsini Goodrich & Rosati*

Ms. Patricia Dunn - *Former Chairman of the Board; Hewlett-Packard Company*

Panel 3

Mr. Mark Hurd - *President, Chief Executive Officer, and Chairman of the Board; Hewlett-Packard Company*

[Link to the Statements, Testimonies, and Transcripts](#)

House Committee on Energy and Commerce – “*Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?*” September 29, 2006

Witnesses:

Panel 1

Mr. Doug Atkin - *Anglo-American Investigations Inc.*

Panel 2

Mr. Christopher Byron - *Journalist; The New York Post*

Panel 3

Mr. Thomas Meiss - *Associate General Counsel; Cingular Wireless*

Mr. Michael Holden - *Litigation Counsel; Verizon Wireless*

Mr. Charles Wunsch - *Vice President for Corporate Transactions and Business Law; Spring Nextel*

Ms. Lauren Venezia - *Deputy General Counsel; T-Mobile USA*

Mr. Greg Schaffer - *Chief Security Officer; Alltel Wireless*

Ms. Rochelle Boersma - *Vice President for Customer Service; U.S. Cellular*

Panel 4

Mr. Joel Winston - *Associate Director, Division of Privacy and Identity; Protection Bureau of Consumer Protection*

Ms. Kris Anne Monteith - *Chief, Enforcement Bureau; Federal Communications Commission*

[Link to the Statements, Testimonies, and Transcript](#)

Hearings Related to Financial Information

House Committee on Banking and Financial Services – “*Use of Deceptive Practices to Gain Access to Personal Financial Information*” July 28, 1998

Witnesses:

Panel 1

Al Schweitzer - *Private Investigator and Security Consultant*

Robert Douglas - *President, Douglas Investigations*

Panel 2

Julie L. Williams - *Acting Comptroller of the Currency*

Mozelle W. Thompson - *Commissioner; Federal Trade Commission*

Jeff Clements - *Assistant Attorney General for the Commonwealth of Massachusetts*

Panel 3

Boris F. Melnikoff - *Senior Vice President; Wachovia Corporation (appearing on behalf of the American Bankers Association)*

Eddy L. McClain - *National Council of Investigation and Security Services*

Robert Glass - *Vice President of National Information Services, LEXIS-NEXIS, appearing on behalf of the Individual Reference Services Group*

Evan Hendricks - *Editor and Publisher, Privacy Times*

Russell Schrader - *Senior Vice President and Assistant General Counsel, VISA*

[Link to the Statements, Testimonies, and Transcripts](#)

[Back to Table of Contents](#)

IV. EXISTING AND PENDING STATE PRETEXTING LAWS

Section 638 of the California Penal Code (Senate Bill 202 of 2006)

Status: Approved by Governor on September 29, 2006. Filed with Secretary of State September 29, 2006. Went into effect January 1, 2007.

Summary: An act to add Section 638 to the Penal Code, relating to privacy.

Language Regarding Pretexting:

SECTION 1. Section 638 is added to the Penal Code, to read:

638. (a) Any person who purchases, sells, offers to purchase or sell, or conspires to purchase or sell any telephone calling pattern record or list, without the written consent of the subscriber, or any person who procures or obtains through fraud or deceit, or attempts to procure or obtain through fraud or deceit any telephone calling pattern record or list shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in a county jail not exceeding one year, or by both a fine and imprisonment. If the person has previously been convicted of a violation of this section, he or she is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in a county jail not exceeding one year, or by both a fine and imprisonment.

[**Link to article discussing Senate Bill 202**](#)

Pending California Legislation – Senate Bill 328 of 2007

Introduced by: Corbett

Date of Introduction: February 16, 2007

Status: Pending

Summary: An act to amend Sections 1798.80 and 1798.84 of, and to add Section 1798.83.5 to, the Civil Code, relating to personal information.

Language Regarding Pretexting:

“This bill includes a telephone calling pattern record or list, as defined, in the definition of personal information" that a business is required to ensure personal privacy. The bill also prohibits any person, as defined, from, among other things, 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, with specified exceptions. The bill provides civil remedies for the violation thereof, and would make related and conforming changes in that regard.”

[Link to Bill Analysis](#)

[Link to California State Senate Documents](#)

[Back to Table of Contents](#)

**V. OVERVIEW AND ANALYSIS OF STATE & FEDERAL
PRETEXTING CASE LAW & PROFESSIONAL ETHICS ISSUES
RELATED TO THE USE OF PRETEXTING BY ATTORNEYS**

**[Fishing With Dynamite - How Lawyers Can Avoid Needless Problems From
“Pretextual Calling” \(Alabama State Bar Magazine\) 2008](#)**

This comprehensive examination of pretexting provides an excellent overview of pretexting. The authors provide a brief review of the Hewlett-Packard scandal as well as a detailed explanation of what “pretexting” actually is. They explore several of the existing laws, including certain IP cases involving pretextual calling, and explain the legal issues of each statute/case individually. The authors also look at some of the limits of pretextual calling and present some guidelines for effectively utilizing pretexting within legal parameters. They conclude by stating, “When engaging in “pretexting,” investigators and the lawyers who hire them should take care to operate within the law and to abide by the relevant rules of professional conduct. Miscalculations can be costly.”

[Understanding Investigative Pretexts 2002](#)

Section and analysis from article:

CASE LAW: FTC v. Rapp, CA 99-WM-783 (D.Col.)

The actions of James Rapp, a private investigator who owned a firm called Touch Tone Information, specializing in pretext investigations, resulted in an indictment and conviction for racketeering, with a 75-day jail sentence and four years of probation. The verdict was handed down in Colorado in January 2000.

Bottom line: Do not use pretext to gain access to banking and financial customer data.

While this may seem like a common sense issue, you cannot legally access someone else's financial records and bank information. This is among the most heavily protected areas of personal privacy. The recently passed Gramm-Leach-Bliley Financial Services Modernization Act specifically makes gaining unauthorized access to banking and financial customer data through pretext a criminal offense.

There are investigators who like to grab all available information when conducting an investigation. This is wasteful, dangerous and unnecessary. While such information may prove useful during an investigation, you might also gain it through previously submitted financial statements, Dun & Bradstreet reports and similar data checks, as well as through conducting interviews. The flip side is the inadvertent creation of a claim for the insured for invasion of privacy - a claim that would likely prevail.

Insurance Claim Information:

Several states, 17 at last count, have adopted some version of the National Association of Insurance Commissioner's Insurance Information and Privacy Protection Model Act (NAIC 670-1), which states:

No insurance institution, agent or insurance support organization shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, a pretext interview may be undertaken to obtain information from a person or institution that does not have a generally or statutorily recognized privileged relationship with the person about whom the information relates for the purpose of investigating a claim where, based upon specific information available for review by the commissioner, there is a reasonable basis for suspecting criminal activity, fraud, material misrepresentation or material non-disclosure in connection with the claim.

Food Lion, Inc. v. Capital Cities/ABC, Inc., 964 F.Supp. 956 (M.D. N.C. 1997)

For those outside Minnesota, pretext remains a viable means for gaining information. This was evidenced in the 1997 Food Lion, Inc. v. Capital Cities/ABC, Inc., 964 F.Supp. 956 (M.D. N.C. 1997) case. Many remember the multi-million-dollar lower court verdict, which was reduced to just \$2 by the 4th Circuit Court of Appeals. While not endorsing pretext, it did establish that the mere use of a ruse was not sufficient to create damages.

Of particular note, the state of Minnesota specifically prohibits any type of pretext in Chapter 72A of the Minnesota Insurance Statute.

Green v. State Farm Fire and Casualty, 667 F.2d 22 (9th Cir. 1982)

The circumstances in this case far exceed the normal pretext. In this instance of suspected arson, the adjuster posed as a state policeman, threatened the insured with prosecution (in the role of adjuster) and implied to neighbors that the insured had set the fire. It is the view of this author that the \$250,000 in punitive damages had more to do with the nature of the ruse and the adjuster's conduct than the mere use of the pretext.

Redner v. Worker's Compensation Appeals Board, 485 P.2d 799 (Cal. 1971)

In this case, the pretext again went far beyond an indirect interview. An investigator induced the claimant to drink to intoxication and then saddle and ride a horse, all the latter of which was videotaped by the investigator. Here, again, the overzealous tactics of the investigator are more in question than the pretext element itself.

As evidence of many courts' permitting pretext as a viable investigative tool, I offer the following:

Turner v. General Adjustment Bureau, 832 P.2d 62 (Utah App 1992)

In this case, investigators were repeatedly invited into the claimant's home while posing as marketing representatives. They only made note of the claimant's comments about her activities and did not videotape her while inside her residence. Videotape was only obtained outside the claimant's residence. As such, the court ruled that the investigators' actions caused no damages because the time inside the house was brief and for a purpose permitted by the claimant.”

[The Truth Behind Pretexting: In-house Investigations and Professional Responsibility Concerns, 2007](#)

By Patrick Arentz (Robins, Kaplan, Miller and Ciresi, LLC)

Excerpt:

“What is Pretexting?”

Pretexting is a practice where an individual lies about her identity in order to obtain confidential or privileged information that she is not entitled to. There are a number of different ways pretexting occurs. Pretexters may use the telephone or computer. They may claim to be an institution like a bank or credit agency, or they may call a company claiming to be the consumer.

Pretexting for financial data is a federal offense under the Gramm-Leach-Bliley Act.^[1] At the time of the H-P scandal, the legality of pretexting for other forms of information, such as for phone records, was considered a legal gray area.^[2] Under federal law, pretexting may fall within the proscriptions of wire^[3] or computer fraud.^[4] And just last May, for example, the Federal Trade Commission, in an attempt to stop pretexting, charged five internet companies with violating Section 5 of the FTC Act, which bars "unfair or deceptive acts" in business practices.^[5] State law crimes involving fraud and identify theft-related statutes may also be used to prosecute pretexters.

On January 12, 2007, the President signed into law the Telephone Records and Privacy Act of 2006.^[6] This new law makes it a federal felony to fraudulently acquire telephone records.^[7] Among other things, the Act makes it a crime to knowingly and intentionally obtain confidential phone records information of a "covered entity" in interstate or foreign commerce by making false or fraudulent statements or representations to an employee of a "covered entity."^[8] The term "covered entity" is defined as all telecommunications carriers, including those providing IP-enabled voice service (voice-over-internet protocol services).^[9] ”

[Electronic Privacy Information Center \(EPIC\) – Letter to Ethics Board Concerning Attorneys' Use of Pretexting 2006](#)

Excerpt:

“In July 2005, EPIC began a campaign to end the practice of "pretexting."^[1] Pretexting is the use of impersonation or fraud to trick another person into releasing personal information. Through pretexting, online data brokers and investigators offer to obtain private calling records, the identities of individuals who use dating services, and the identities of people who use P.O. Boxes. Many of these services are advertised online for any member of the public to buy data on others.

EPIC identified dozens of websites that offered to obtain personal information through pretexting, and submitted a list of 40 such sites to the Federal Trade Commission for

investigation.^[2] We also petitioned the Federal Communications Commission to protect individuals' phone records from pretexting.^[3]

In the course of investigating pretexting, it has become increasingly clear that attorneys are major consumers of pretexting services... We believe that pretexting is incompatible with ABA Model Rules 1.2, 3.4, 4.1, 4.4, and 8.4. We provide documentation below of the mounting evidence showing that attorneys are purchasing the services of pretexters, and urge you to take action to prevent attorneys from using pretexting services.”

[Back to Table of Contents](#)

VI. POSITIONS OF THE PRIVATE INVESTIGATIONS COMMUNITY AND REGULATORS ON PRETEXTING

National Council of Investigation & Security Services (NCISS)

- [NCISS Position Statement on the Acquisition and Use of Telephone Records](#)
- The NCISS website has several articles concerning pretexting and its use in investigations:
 - [Pretexting: A Case of Mistaken Identity](#)
 - [An Ethical Look at Pretexting by Kitty Hailey, CLI*](#)

Federal Trade Commission

- [FTC: Facts for Consumers “Pretexting: Your Personal Information Revealed”](#)
- [The FTC on Pretexting: The PI Magazine Interview with Joel Winston; Jan/Feb 2005](#)

International Association of Security and Investigative Regulators

- In 2006, IASIR issued the following resolution:

"Be it resolved that IASIR recognizes the common practice of pretext as an investigative tool in lawful investigations by both public law enforcement and licensed private investigators and security practitioners."

State Licensing Agencies

The following is a comprehensive list of all fifty states' requirements and licensing agencies that are required for private investigators: http://www.nciss.org/Links/State_Licensing_Agencies.htm. The list indicates there are ten states that do not require private investigators to be licensed statewide. Some cities in a few of these states require licenses to offer private investigation services, some only require business licenses, and the remainder do not regulate the private investigation business at all.

[Back to Table of Contents](#)

VII. PRESS REPORTS OF PRETEXTING SCANDALS

Portfolio.com

Diary of a Short-Seller (2008)

Excerpt: “Einhorn was investigated by the S.E.C., and documents related to his Allied speech and positions were subpoenaed. (Then-New York attorney general Eliot Spitzer’s office also looked into Einhorn’s activities but took no action.) One of the S.E.C.’s lawyers eventually left and registered as an Allied lobbyist. Through pretexting—pretending to be someone else—an Allied investigator went on to snatch Einhorn’s phone records, a case that generated much less attention than a similar breach at Hewlett-Packard that involved pretexting journalists. (Allied eventually admitted to having the records but denied authorizing pretexting.)”

Toyota Sued For Cell Phone Pretexting (2008)

Excerpt: “A former employee of Toyota's Georgetown, Kentucky plant has sued the auto maker, one of Kentucky's largest employers, for accessing his personal cell phone records by using a technique called pretexting during an internal investigation at the Georgetown plant in 2005. Although federal law requires that the owner of a cell phone must give permission before any third party accesses the owner's cell phone records, the employee, Charles W. Jones, Jr., has stated in court documents that he did not give Toyota permission to access his records.”

Belfair couple pleads guilty in nationwide identity-theft conspiracy (2008)

Excerpt: “The Mason County couple who prosecutors say were key players in a "pretexting" conspiracy among private investigators from Texas to New York have pleaded guilty to conspiracy, wire fraud and aggravated identity theft in federal court.

Emilio Torrella, 36, and his wife, Brandy, 27, of Belfair, admitted Tuesday to a scheme to illegally obtain confidential information on citizens for law firms, insurance companies and collection agencies.

The Torrellas are owners of BNT Investigations, which federal prosecutors say was at the center of a nationwide investigation prosecutors dubbed "Operation Dialing for Dollars." The investigation targeted private investigators who lied to government agencies, including the

Social Security Administration and Internal Revenue Service, to obtain confidential information on citizens.”

Liar, Liar, and Pretexting (2006)

Excerpt: “Some of the cases brought by the government under consumer protection statutes have been downright nasty. In 1999 for example, the FTC fined James and Regena Rapp \$200,000 for pretexting after James Rapp reportedly wrote a 1000 page book about how to obtain information, and reportedly obtained private information on people like Monica Lewinsky, the Ramsey family, and others - usually at the behest of private investigators. In another case in 2003, a man contacted an Internet based company called Docusearch.com to find out information about his former girlfriend. He purchased various services from the online company, including her address, social security number, employer information including employer’s address. Docusearch hired an investigator, Michele Gambino to find this information, which she did by “pretexting” the ex-girlfriend. For a few hundred dollars, the ex boyfriend located his ex-girlfriend, found her, and killed her, before killing himself. Her estate sued Docusearch, and the court found that the pretexting was a deceptive trade practice. In another case, Massachusetts v. Source One, Source One advertised in a bunch of legal periodicals that it would conduct “asset searches” for a fee. Lots of lawyers used their services to find out whether people they were suing (or about to sue) had any assets worthy of attachment - after all, you don’t want to sue unless you can collect, right? Problem was, as everybody knows (or should know) financial records are presumably secret. A host of government regulations, including the Gramm Leach Bliley Act (GLBA), and Office of the Comptroller of the Currency and other financial regulations prohibit financial institutions from disclosing this information except under certain circumstances - and helping out private investigators [isn’t] one of those recognized exceptions (that is, without a subpoena).”

FTC Permanently Halts 'Pretexting' Scheme (2008)

Excerpt: The Federal Trade Commission has put a permanent halt to an operation that allegedly obtained consumers’ confidential phone records without their knowledge or consent and sold them to third parties... This is the latest in a series of FTC cases targeting telephone pretexters – individuals who use false pretenses to obtain consumers’ confidential information.

Since 2006 the FTC has charged sixteen individuals and their corporations with violating federal law by pretexting to obtain phone records of third parties. All have now been barred from pretexting and all have been ordered to give up the money they made engaging in the illegal practice.

In February 2007, the FTC asked a U.S. district court to order a permanent halt to the operations of a company that sold consumers' confidential phone records, including information on calls placed and received. The FTC also sued the individuals who had used false pretenses to obtain the records from phone companies and then supplied those records to the company for a fee. The agency alleged these practices were unfair and deceptive in violation of federal law, and could endanger consumers' safety. The agency also asked the court to order the defendants to give up their ill-gotten gains.”

[Back to Table of Contents](#)