Testimony of

Robert Douglas

CEO
PrivacyToday.com
April 13, 2005

Testimony of Robert Douglas
CEO, PrivacyToday.com
Before the
United State Senate Committee on the Judiciary
--
Hearing on
Securing Electronic Personal Data: Striking a Balance
Between Privacy and Commercial and Governmental Use
--
April 13, 2005

My name is Robert Douglas and I am the CEO and founder of PrivacyToday.com located in Steamboat Springs, Colorado. I provide consultation to the private and public sectors on issues involving all aspects of identity theft, identity fraud, and personal information security. During the past eight years my work has centered on assisting the financial services industry, the general business community, government, and law enforcement agencies to better understand the scope and methodology of identity crimes through educational materials, presentations, auditing, and consultation.

I have provided consultation and expert testimony for civil and criminal investigations brought by private parties and state and federal law enforcement agencies. Most relevant to today's hearing, I served as a consultant and expert witness for the Federal Trade Commission in the design and execution of Operation Detect Pretext, a sting operation to catch and civilly prosecute individual and corporate offenders participating in the illegal "information broker" industry. I served as an expert witness to the Florida Statewide Grand Jury on Identity Theft. I served as an expert witness and consultant for the plaintiffs in a federal civil action brought by the parents of Amy Boyer, a young woman slain in a murder committed by a man who purchased Ms. Boyer's social security number, date of birth, and place of employment from a web-based information broker. I have lectured before local, state, federal and international law enforcement associations on the topic of identity crimes. I have been a private investigator and security consultant for the past twenty-two years. This is my fifth appearance before the United States Congress to discuss personal information security.

The Murder of Amy Boyer

Far too often as we grapple with the issue of balancing the privacy of Americans with the necessary and legitimate uses of Americans' personal information the debate centers on discussions of "data", but not the lives behind the "data". In order to illustrate what I've learned over the course of more than twenty years using and investigating the good and harm of database information, I'd like to begin by focusing on one life behind one set of data. The untimely and violent end to that life encapsulates all the issues that surround securing personal information while balancing privacy with legitimate uses of information. Further, investigating this one act of violence led me to a more complete understanding of how personal information is being used and abused in the United States today. This case also demonstrates that the problem is much larger than the recent ChoicePoint breach and other instances that have recently been in the headlines. The problems of securing personal information and balancing privacy with legitimate use are intertwined and impact every business and government sector.

On a quiet fall afternoon in October of 1999 Amy Boyer, a young Nashua, New Hampshire woman, was leaving work with two co-workers. The small group was discussing plans for that weekend as they walked to their cars parked on a side street less than a block from the office. As Amy said good-bye and closed her door, a car driven by Liam Youens

sped up the street and stopped driver's door to driver's door with Amy's car. Youens yelled out Amy's name as he fired 11 bullets into the head and upper body of his unsuspecting 20 year-old victim. Youens then fired one last shot into his head, instantly killing himself as Amy lay just feet away mortally wounded.

Liam Youens was a demented young man. He glorified the Columbine killers and toyed with the idea of doing the same at Nashua High School. He openly planned Amy's murder and the intended murder of others for more than a year. The reason we know so much about Youens is that he documented his plans to murder Amy on a web site he created to publish his sick desires.

But that web site contained far more than just the perversity of Liam Youens. It contained the starting point for a trail of evidence that proves how personal information of all Americans stored with good intent in myriad databases across this country can be easily obtained and used for incalculable harm. The trail that began on a quiet Nashua street led to the shadowy world where a small but persistent number of illegitimate information brokers and private investigators, in addition to a growing number of identity thieves and other criminals, access databases holding our most important personal information and use that data for criminal purposes.

In Amy's murder the evidence showed that Youens decided to ambush Amy as she left work. But Youens had a problem. He didn't know where Amy worked. So he started using information brokers and private investigators that run Internet based operations that specialize in obtaining and selling personal information on Americans. In separate Internet transactions Youens purchased Amy's date of birth, social security number, home address, and finally her place of employment.

Youens himself was struck by how easily he was able to purchase Amy's personal information while concealing his evil intent. Here is a small sampling of Youens own words from his web site where he was documenting his step-by-step activities to locate and kill Amy:

When I finished finding [street name redacted] residents in the phone book I thought my best bet was apt. number 7 so I entered the information. It wasn't 7, but who cares I got a HIT! I fell to the floor and let the endorphines fly. Her address was [residential address redacted] she didn't move from home yet, no other information was provided in the background check.

I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment. It's accually obsene what you can find out about a person on the internet. I'm waiting for the results. [typos from original/redaction and emphasis added by R. Douglas]

The Internet site Youens found to get Amy's "current employment" and "everything else under the Sun" was Docusearch.com. To obtain Amy's "current employment" Docusearch provided Amy's social security number, date of birth, and home address to Michele Gambino, another private investigator/information broker operating as Gambino Information Services out of New York City. Gambino has at times described her specialty as "proper pretext", "subterfuge phone calls", or "informative telephone conversations". Those are nice titles for deceit, fraud, and lying. In short, Gambino uses lies to deceive people out of personal information.

At the time of Amy's murder, Gambino and others who worked as subcontractors for Docusearch specialized in defeating the information security systems of financial institutions (including many of the nation's largest banks and brokerage houses), telecommunications companies (obtaining non-published phone numbers and records of phone numbers dialed from any phone in the country), utility companies (power/cable/gas/water/satellite firms all maintain databases of personal information), and unsuspecting private citizens with information about loved ones.

In this case, Gambino conducted a "pretext" to obtain Amy's work address by impersonating an insurance company representative and falsely stating that she had a refund for Amy. By having Amy's social security number, date of birth, and home address, Gambino was able to sound authoritative as most Americans wrongly believe that only someone with legitimate access and authority would have their social security number and other personal information. Gambino was able to deceive Amy and/or Amy's mother out of Amy's work address on the pretext that the work address was needed to process the insurance refund.

The reality is, as far as Docusearch and Gambino were concerned, obtaining Amy's work address by fraud was just another transaction to put money in their pockets. And a lucrative business it is. With just two employees and a handful of independent contractors like Gambino, Docusearch was grossed over $1 Million per year selling and re-selling Americans' personal information.

Outrageously, while Docusearch was in the business of accessing and stealing Americans' personal information and continues to this day to brag about how they can find anything about anybody, neither Gambino nor Docusearch took any constructive steps to determine who Youens was, much less why he needed the employment address of Amy. Had Docusearch or Gambino simply typed Amy's name into any free search engine they would have found Youens' web site documenting his intent to kill Amy.

Docusearch was on notice that their Internet site was being used by potential stalkers with intent to do harm. Just days before Gambino used a "pretext" to obtain Amy's work address, Docusearch learned that another "client" was attempting to obtain an address on a young woman in Texas for potential harm. In the Texas case, Docusearch was once again using a pretext to learn the address of the young woman from the woman's mother. Fortunately, the mother was savvy enough to realize they were trying to deceive her out of her daughter's address and told the Docusearch "investigator" that her daughter had a restraining order against Docusearch's client.

While Docusearch, Gambino, and others in the information brokerage and investigative fields often argue that they shouldn't be held responsible for the unforeseen consequences of selling "data", those defenses ring hollow. Not only is there ample evidence in the files of Docusearch and Gambino of potential harm caused by the personal information they are selling on demand, the information brokerage/private investigative industries have been aware since at least the early 1980s of criminals using their services to carry out violent and non-violent crimes.

Congress Passed the DPPA and Other Statutes to Protect Americans

In March of 1982 the information broker/private investigative professions and all who maintain databases with personal information learned first-hand that personal information in the wrong hands can lead to severe physical harm or murder. In a scenario frighteningly similar to what happened to Amy, actress Theresa Saldana was repeatedly stabbed and slashed by a stalker at the front door of her home. To find Saldana, the stalker hired a private investigator to obtain Saldana's mother's non-published phone number. The stalker then called Saldana's mother and tricked her into providing Saldana's home address by using the "pretext" that he was Martin Scorcese's assistant and needed Saldana's home address in order to reach Saldana for a movie role.

Following the Saldana attack, came the 1989 murder of actress Rebecca Schaeffer. In that case, a private investigator obtained Schaeffer's home address through the California motor vehicle database and sold the address to a stalker. The stalker used the address information to stalk and kill Schaeffer. The attack of Saldana and the murder of Schaeffer, combined with a growing body of evidence that personal information contained in state motor vehicle records (at that time routinely provided to anyone requesting it) was being used for criminal purposes, led to passage of the Drivers Privacy Protection Act (DPPA). A federal law that I would argue is violated thousands of times each day.

But the trail of evidence in Amy's murder does not end with an obsessed killer and a couple of greedy private investigators operating Internet information brokerages. Quite simply, the evidence in Amy's murder leads to thousands of documents demonstrating in real time how databases maintained in a wide range of American businesses and entire industries that contain our most personal information are breached everyday.

Commercial/Government Information Security Systems Are Breached Every Day

On a daily basis Docusearch, Gambino, and other associates of Docusearch were penetrating the information security systems of this nation's financial services industry, postal service, telecommunication and other utility companies, and selling that personal information to just about anyone. Contained within the files of Docusearch, Gambino, and hundreds of other similar companies is evidence that not only can any piece of information about anybody or any company be obtained by anyone willing to pay for it, but clear and convincing evidence that when it

comes to being guardians of critical personal information both government and commercial entities deserve a failing grade.

Unfortunately, Docusearch and Gambino are not rare examples that limit the scope of the problem to a finite few. The reality is there are hundreds of "Docusearchs" combined with thousands of identity thieves conducting arguably tens of thousands of breaches of information security systems across all business and government sectors each day in this country. You don't get ten million identity theft victims and fifty-plus billion dollars in losses to identity theft related financial fraud from dumpster divers.

To further illustrate the scope of the problem, consider what we already know when it comes to the black market of personal information provided by unscrupulous information brokers and private investigators. Remember, these unscrupulous companies are a window into the very same methods used by criminals, identity thieves, and potentially terrorists.

Federal Trade Commission's Operation Detect Pretext

Following my second of two appearance before the House Banking Committee , in which I assisted the Committee with a surreptitious survey of online Internet information brokers and their offerings that confirmed financial information of Americans was for sale, I worked with the Federal Trade Commission to design a sting operation to civilly prosecute Internet based information brokers selling financial account information (including specific account numbers and balances) in violation of the Gramm-Leach-Bliley Act. Operation Detect Pretext, as it was named, revealed that there were hundreds of Internet based information brokers and private investigators advertising the sale of Americans' most personal information in violation of any of a number of federal statutes including but not limited to Gramm-Leach-Bliley, the FCRA, the DPPA, and the Unfair and Deceptive Trade Practices Act. There was also evidence in the files of at least one of the FTC targeted information brokers of the broker selling personal information (perhaps unknowingly) to identity thieves.

The reality of how the Docusearchs, Gambinos, and identity thieves (as we know from the recent ChoicePoint case) defeat the information security systems of so many companies is that they often begin by acquiring the personal information of the victim of the intended crime. Using this personal information the criminal or unscrupulous information broker can impersonate the victim in order to obtain further personal information or carryout a criminal act by convincing the rightful custodian of personal information to reveal it to the criminal posing as the victim.

As an information broker once explained the process to me:
1) Know what piece of data you want.
2) Know who the custodian of the data is.
3) Know who the custodian will release the data to.
4) Know what circumstances are needed for the release of the data.
5) Become (impersonate) that person with those circumstances.

Illegitimate Subscriber Access - The Resale Market

Unfortunately, many of the illicit information brokers who will steal and sell any information about anybody have subscriber access (through a variety of legitimate and illegitimate means) to the legitimate information brokerage companies. They need the biographical information contained in the databases of the legitimate information brokers in order to carry out their pretexts like Gambino did to Amy. Specifically, to carry out the 5 steps outlined above, the unscrupulous information broker, private investigator or identity fraud criminal will purchase the biographical data needed (from either a legitimate information broker via a fraudulent subscriber agreement as in the instant ChoicePoint case, or via a reseller who obtains the information from a legitimate broker and willingly violates the no resale contract) in order to impersonate an individual that desired information will be released to.

There are a number of information brokerage companies, in addition to ChoicePoint, that have maintained relationships with information brokers and private investigators that I classify as resellers. While ChoicePoint and several other brokers have announced they will further restrict access to full social security numbers, dates of birth, and other personal identifiers to some clients of certain size and business lines, there is no doubt that absent

legislation other companies will step in to fill the void--even if the ChoicePoint-styled self-remedy is effective. The hottest topic in the private investigative and information brokerage fields right now is where can you obtain full social security numbers and from what companies. The information resellers and investigative markets will flock from ChoicePoint to other mainstream information brokers willing to accept the revenue until Congress acts.

Indeed, for many years information resellers have easily deceived the major information brokers in the application process or violated the no resale clauses of their contracts. This is the worst kept secret in the information broker/investigative world.

Information Security in the U.S. is Laughable at Best

But even if all legitimate information brokers were to appropriately and effectively secure the data in their electronic warehouses, the flow of information would continue. Criminals and others will just access, and in many cases continue to access, databases from the government and private sector to find the personal information they need for their crimes.

When it comes to the overwhelming majority of databases in this country from government maintained military, postal, education, tax, welfare, and child support records to commercially maintained financial account, telecommunications, utility, medical, and business records, the information can almost always be obtained by an individual named in the records. Often this is the actual account holder. For the unscrupulous information broker or criminal, it is merely a matter of piecing together enough personal information about the targeted victim to impersonate the victim to the custodian of the information. And with far too much frequency, the key to unlocking most personal information is the social security number.

As I demonstrated a week ago in a story by Jonathan Krim of the Washington Post, it is a simple matter to go on the Internet and purchase from any one of a number of information brokers the social security number of any American. But even if social security numbers were not easily obtained from information brokers through direct or indirect (the illicit resale market), the indisputable fact is social security numbers have been compromised in this country in many ways for such a long period that it is laughable that either government or commercial enterprises use the number as a personal identifier for maintaining security of databases.

Yet this is the method chosen by more than 50% of the nation's banks, telecommunication companies, hospitals, doctor's offices, universities, utility providers, government programs, and almost any government or commercial entity one can name. I can inform this Committee and easily prove to this Committee based upon my experience investigating and studying information security practices and criminal methods for defeating those practices, and from the documents available in the Boyer murder case (that I would gladly share with this Committee in a closed setting), that any information security system using personal biographical information as the primary security identifier to allow access to the information is a fatally flawed system.

Congress Should Outlaw the Use of
Personal or Biographical Identifiers for Information Access

Let me blunt. If this Committee and this Congress want to take a giant step down the road to securing Americans' data stored across all government and commercial entities, that step should be to prohibit the use of social security numbers, dates of birth, addresses, phone numbers, mothers maiden name, and any other personal biographical identifiers as information access security protocols. The reason for prohibiting the use of personal biographical information as security protocols for access to information maintained in databases is simple. Anyone can find them for free or buy them in hundreds of locations and databases across the country and on the Internet.

Why is it critical that we maintain the security of these databases? Because the vast majority of personal information contained in databases across this country is used for purposes that benefit Americans every day. Those benefits include commercial applications that assist citizens in transactions that weren't possible even ten years ago, but that we now take for granted. Additionally, the personal and biographical data maintained in a wide range of storage methods can be of critical value for government in fulfilling constitutionally mandated societal welfare, law

enforcement, military, and national security functions. In the commercial sector personal information databases can assist in expediting transactions resulting in lower costs in addition to fraud prevention, detection, and prosecution.

The challenge is to determine a way to maintain this information which can be used for good and harm in a secure way that guarantees it is available for good, but not harm. As with any challenge, we must first understand the scope of the problem.

As I've tried to demonstrate through the evidence uncovered in the Boyer murder case, the scope of the problem far exceeds the ChoicePoints of the world. I am not here to make excuses for ChoicePoint or the other "legitimate" information brokers who after all do provide critical information to government and the private sector as discussed above.

In fact, I think the most recent breach that was the catalyst for this hearing is inexcusable given ChoicePoint's prior knowledge of attempts to fraudulently obtain subscriber access.

Legislation Must Address All Commercial and Government Entities

Yet to limit any proposed legislation to the information broker industry would be short-sighted in my opinion. After all, information brokers are nothing but aggregators of data contained in a wide variety of storage media. From courthouses; state, local, and federal offices; and, the military to marketing lists; phone directories; credit bureaus; insurance companies; and, dozens of commercial industries, information brokers gather "data" that is re-packaged and sold for a wide variety of uses.

If Congress takes action that only affects the commercial information broker industry while ignoring the government and the private business sector databases where information brokers obtain their raw data, there will be little accomplished. This is because criminals and others who would use information for illegal purposes will turn to the original sources of that raw information.

To place the question as to scope of the problem and how to curb it in the framework of the recent ChoicePoint breach, ask the following question: What good is to mandate that ChoicePoint have adequate security protocols to protect our personal information if the banks, telecommunication companies, universities, hospitals, doctors offices, insurance companies, utility providers, car dealers, and governmental agencies don't have adequate security protocols and are as porous when it comes to information security as ChoicePoint was?

If the ChoicePoint debacle causes this Committee and Congress to begin to seriously re-think how we protect all forms of data in this country, particularly at a time of war when our enemies have proven adept at understanding and using to their advantage information systems (such as deficiencies in driver's license cross-reference verification systems that allowed issuance of multiple driver's licenses from multiple jurisdictions to the 19 September 11th hijackers) then a complete understanding will be needed of how information too easily accessed and used for harm can be secured across the board and used for the benefit of individuals and the security of the nation.

But it must be a holistic approach. There are far too many sources of personal information in this country to either believe we can put the genie back in the bottle when it comes to social security numbers and other personal biographical identifiers or that we can solve the problem of securing information by addressing industries on a piecemeal basis.

In fact, Congress has tried the piecemeal approach for years with different issues, governmental agencies, and commercial industries. From the Privacy Act (restrictions on government use of personal information) to the Fair Credit Reporting Act (restrictions on consumer reporting agencies use of personal information) to the Driver's Privacy Protection Act (restrictions on state motor vehicle agencies handling of personal information) to most recently Gramm-Leach-Bliley (restrictions on financial institutions use and handling of personal information) Congress has addressed issues of privacy, data protection and data access on a case by case basis.

I would urge this body to recognize and accept as fact that many of the same challenges when it comes to securing personal data while balancing the legitimate privacy of Americans with the legitimate needs of government and beneficial commercial practices permeate all aspects of American government and private business. It is time to mandate that all government entities and the business community develop practical and effective information security programs that address 1) appropriate use questions (who gets access) and 2) authentication issues (how access is granted in a secure method).

If we don't take this approach across all sectors, criminals and this nation's enemies will do just as the unscrupulous and illegitimate information brokers I've discussed throughout this testimony do should they be effectively cut off from access in one database. They'll just turn to the next database in the next industry that has not been protected.

Need For A GAO Investigation

I have seen a number of investigations done by the GAO which provide a blueprint for an investigation this Committee might find beneficial as it grapples with the issues at hand. The two most relevant investigations were: 1) An investigation as to how easily undercover GAO investigators using movie prop badges and fake law enforcement IDs created with off the shelf software were able to access secure government facilities and secured areas of airports; and, 2) An investigation as to how easily undercover GAO investigators were able to obtain state issued driver's licenses by submitting obviously fraudulent identity documents to counter clerks.

Perhaps this Committee would consider requesting the GAO to perform an investigation of how easily they can access telecommunication company databases; financial services companies databases; utility companies databases; hospital databases; university databases; and, state and federal government agency databases, all by means of social engineering/pretext. I think the results would be enlightening.

Oversight and Enforcement Are Critical

Additionally, Congress needs to exercise oversight on the agencies already charged with enforcing the FCRA, GLBA, DPPA, and other applicable privacy and data security laws. From credit reports, to financial account information, to driver's records and beyond--it is all for sale by hundreds of companies routinely laughing in the face of Congress and the laws that are not enforced.

Those laws were passed with reasons that were important at the time, but are even more important in the age of terrorism that has been visited upon our shores. Our porous information systems in this country are a terrorists dream and a potential terrorist tool. It is time we get serious about protecting information of all forms in this nation.

In addition to the dangers of criminals, terrorists, identity thieves, and illicit information brokers who violate Americans' privacy there is an equally compelling reason to take action to protect personal information. The very same information that is too often abused is the life blood of this country and all Americans. If Americans don't have faith that the information they provide is secure it will harm commerce, and more fundamentally, the trust we all place in those that we share our most important and private data with.

In closing, I'd like to make an offer to this Committee, any other Committee of the Congress, any individual Senator of Representative, or any agency of the United States government. I will gladly volunteer my time and resources, including the information and evidence I've gathered over the last 8 years, to provide as much assistance as I can to securing the personal information of Americans.

Thank you.

APPENDIX I

I have testified before the United States Congress on four previous occasions. The July 28, 1998 Hearing on "The Use of Deceptive Practices To Gain Access To Personal Financial Information" (U.S. House of Representatives Committee on Banking and Financial Services); the April 12, 2000 Hearing on "Establishing a Commission For the Comprehensive Study of Privacy Protection" (U.S. House of Representatives Committee on Government Reform, Subcommittee on Government Management, Information and Technology); the September 13, 2000 Hearing on "Identity Theft and Related Financial Privacy Issues" (U.S. House of Representatives Committee on Banking and Financial Services); and, the September 9, 2003 Hearing on "Homeland Security Threats Posed By Document Fraud, Identity Theft, and Social Security Number Misuse" (U.S. Senate Committee on Finance).

In addition to my previous testimonies before Congress, I served as a consultant and expert witness for the Federal Trade Commission in the preparation and execution of Operation Detect Pretext, a sting operation designed to catch and prosecute individual and corporate offenders participating in the illegal "information broker" industry. I also served as an expert witness to the Florida Statewide Grand Jury on Identity Theft. I continue to serve as an expert witness and consultant for the plaintiffs in a federal civil action brought in New Hampshire by the parents of Amy Boyer, a young woman slain in a murder/suicide committed by a man who purchased Ms. Boyer's social security number, date of birth, and place of employment from a web-based information broker. I have lectured before local, state, federal and international law enforcement associations on the topic of identity crimes.

To assist the private sector and the financial services industry in its efforts to detect and combat financial crimes involving identity theft, I have authored a number of training guides including: "Privacy and Customer Information Security - An Employee Awareness Guide" (2001); and, "Spotting and Avoiding Pretext Calls" (2000). I have served as a keynote speaker for the FDIC and I have been a frequent lecturer at state and national banking association conferences.

Finally, prior to founding American Privacy Consultants, Inc., I was a Washington, D.C. private detective specializing in criminal defense investigation. I have worked cases involving murder, international terrorism (including conspiracy to murder U.S. nationals and hijacking), political corruption, and government fraud. I have twice been appointed by the U.S. District Court for Washington, D.C. to serve as criminal defense investigator in matters involving international terrorism by members of known Islamic terrorist organizations.

For a complete curriculum vitae see http://www.privacytoday.com/douglas.htm

APPENDIX II

NOTICE: This opinion is subject to motions for rehearing under Rule 22 as well as formal revision before publication in the New Hampshire Reports. Readers are requested to notify the Reporter, Supreme Court of New Hampshire, One Noble Drive, Concord, New Hampshire 03301, of any editorial errors in order that corrections may be made before the opinion goes to press. Errors may be reported by E-mail at the following address: reporter@courts.state.nh.us. Opinions are available on the Internet by 9:00 a.m. on the morning of their release. The direct address of the court's home page is: http://www.courts.state.nh.us/supreme.

THE SUPREME COURT OF NEW HAMPSHIRE

_____

U.S. District Court
No. 2002-255
HELEN REMSBURG, ADMINISTRATRIX OF THE ESTATE OF
AMY LYNN BOYER
v.
DOCUSEARCH, INC., d/b/a DOCUSEARCH.COM & a.
Argued: November 14, 2002
Opinion Issued: February 18, 2003

Gottesman and Hollis, P.A., of Nashua (David A. Gottesman and Anna Barbara Hantz on the brief, and Mr. Gottesman orally), for the plaintiff.

Getman, Stacey, Tamposi, Schulthess & Steere, PA, of Bedford (Andrew R. Schulman and Dona Feeney on the brief, and Mr. Schulman orally), for defendants Docusearch Inc., Wing and a Prayer, Inc. and Daniel Cohn.

Law Office of Hess & Fraas, of Bow (Carol L. Hess on the brief), for defendant Kenneth Zeiss.

Sichenzia Ross Friedman & Ference, of New York, New York (Steven B. Ross on the brief), and Brennan Caron Lenehan & Iacopino, of Manchester (Michael J. Iacopino on the brief and orally), for defendant Michele Gambino.

Chris J. Hoofnagle & a., of Washington, D.C., by brief, for the Electronic Privacy Information Center, as amicus curiae.
Scott H. Harris, of Manchester, by brief, for the New Hampshire Trial Lawyers Association, as amicus curiae.
John M. Healy and Jordan G. Ulery, appearing pursuant to Supreme Court Rule 33(2), by brief, for the New Hampshire League of Investigators, Inc., as amicus curiae.

DALIANIS, J. Pursuant to Supreme Court Rule 34, the United States District Court for the District of New Hampshire (Barbadoro, C.J.) certified to us the following questions of law:
1. Under the common law of New Hampshire and in light of the undisputed facts presented by this case, does a private investigator or information broker who sells information to a client pertaining to a third party have a cognizable legal duty to that third party with respect to the sale of the information?
2. If a private investigator or information broker obtains a person's social security number from a credit reporting agency as a part of a credit header without the person's knowledge or permission and sells the social security number to a client, does the individual whose social security number was sold have a cause of action for intrusion upon her seclusion against the private investigator or information broker for damages caused by the sale of the information?
3. When a private investigator or information broker obtains a person's work address by means of a pretextual telephone call and sells the work address to a client, does the individual whose work address was deceitfully obtained have a cause of action for intrusion upon her seclusion against the private investigator or information broker for damages caused by the sale of the information?
4. If a private investigator or information broker obtains a social security number from a credit reporting agency as a part of a credit header, or a work address by means of a pretextual telephone call, and then sells the information, does the individual whose social security number or work address was sold have a cause of action for commercial appropriation against the private investigator or information broker for damages caused by the sale of the information?
5. If a private investigator or information broker obtains a person's work address by means of a pretextual telephone call, and then sells the information, is the private investigator or information broker liable under N.H. Rev. Stat. Ann. § 358-A to the person it deceived for damages caused by the sale of the information?
For the reasons expressed below, we respond to the first, second and fifth questions in the affirmative, and the third and fourth questions in the negative.

I. Facts
We adopt the district court's recitation of the facts. Docusearch, Inc. and Wing and a Prayer, Inc. (WAAP) jointly own and operate an Internet-based investigation and information service known as Docusearch.com. Daniel Cohn and Kenneth Zeiss each own 50% of each company's stock. Cohn serves as president of both companies and Zeiss serves as a director of WAAP. Cohn is licensed as a private investigator by both the State of Florida and Palm Beach County, Florida.
On July 29, 1999, New Hampshire resident Liam Youens contacted Docusearch through its Internet website and requested the date of birth for Amy Lynn Boyer, another New Hampshire resident. Youens provided Docusearch his name, New Hampshire address, and a contact telephone number. He paid the $20 fee by credit card. Zeiss placed a telephone call to Youens in New Hampshire on the same day. Zeiss cannot recall the reason for the phone call, but speculates that it was to verify the order. The next day, July 30, 1999, Docusearch provided Youens with the birth dates for several Amy Boyers, but none was for the Amy Boyer sought by Youens. In response, Youens e-mailed Docusearch inquiring whether it would be possible to get better results using Boyer's home address, which he provided. Youens gave Docusearch a different contact phone number.
Later that same day, Youens again contacted Docusearch and placed an order for Boyer's social security number (SSN), paying the $45 fee by credit card. On August 2, 1999, Docusearch obtained Boyer's social security number from a credit reporting agency as a part of a "credit header" and provided it to Youens. A "credit header" is typically provided at the top of a credit report and includes a person's name, address and social security number. The next day, Youens placed an order with Docusearch for Boyer's employment information, paying the $109 fee by credit card, and giving Docusearch the same phone number he had provided originally. Docusearch phone records indicate that Zeiss placed a phone call to Youens on August 6, 1999. The phone number used was the one Youens had provided with his follow-up inquiry regarding Boyer's birth date. The phone call lasted for less than one minute, and no record exists concerning its topic or whether Zeiss was able to speak with Youens. On August 20, 1999, having received no response to his latest request, Youens placed a second request for Boyer's employment information, again paying the $109 fee by credit card. On September 1, 1999, Docusearch refunded Youens' first payment of $109 because its efforts to fulfill his first request for Boyer's employment information had failed.

With his second request for Boyer's employment information pending, Youens placed yet another order for information with Docusearch on September 6, 1999. This time, he requested a "locate by social security number" search for Boyer. Youens paid the $30 fee by credit card, and received the results of the search - Boyer's home address - on September 7, 1999.

On September 8, 1999, Docusearch informed Youens of Boyer's employment address. Docusearch acquired this address through a subcontractor, Michele Gambino, who had obtained the information by placing a "pretext" telephone call to Boyer in New Hampshire. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information. Gambino had no contact with Youens, nor did she know why Youens was requesting the information.

On October 15, 1999, Youens drove to Boyer's workplace and fatally shot her as she left work. Youens then shot and killed himself. A subsequent police investigation revealed that Youens kept firearms and ammunition in his bedroom, and maintained a website containing references to stalking and killing Boyer as well as other information and statements related to violence and killing.

II. Question 1

All persons have a duty to exercise reasonable care not to subject others to an unreasonable risk of harm. See Walls v. Oxford Management Co., 137 N.H. 653, 656 (1993). Whether a defendant's conduct creates a risk of harm to others sufficiently foreseeable to charge the defendant with a duty to avoid such conduct is a question of law, Iannelli v. Burger King Corp., 145 N.H. 190, 193 (2000), because "the existence of a duty does not arise solely from the relationship between the parties, but also from the need for protection against reasonably foreseeable harm." Hungerford v. Jones, 143 N.H. 208, 211 (1998) (quotation omitted). Thus, in some cases, a party's actions give rise to a duty. Walls, 137 N.H. at 656. Parties owe a duty to those third parties foreseeably endangered by their conduct with respect to those risks whose likelihood and magnitude make the conduct unreasonably dangerous. Hungerford, 143 N.H. at 211.

In situations in which the harm is caused by criminal misconduct, however, determining whether a duty exists is complicated by the competing rule "that a private citizen has no general duty to protect others from the criminal attacks of third parties." Dupont v. Aavid Thermal Technologies, 147 N.H. 706, 709 (2002). This rule is grounded in the fundamental unfairness of holding private citizens responsible for the unanticipated criminal acts of third parties, because "[u]nder all ordinary and normal circumstances, in the absence of any reason to expect the contrary, the actor may reasonably proceed upon the assumption that others will obey the law." Walls, 137 N.H. at 657-58 (quotation omitted).

In certain limited circumstances, however, we have recognized that there are exceptions to the general rule where a duty to exercise reasonable care will arise. See Dupont, 147 N.H. at 709. We have held that such a duty may arise because: (1) a special relationship exists; (2) special circumstances exist; or (3) the duty has been voluntarily assumed. Id. The special circumstances exception includes situations where there is "an especial temptation and opportunity for criminal misconduct brought about by the defendant." Walls, 137 N.H. at 658 (quotation omitted). This exception follows from the rule that a party who realizes or should realize that his conduct has created a condition which involves an unreasonable risk of harm to another has a duty to exercise reasonable care to prevent the risk from occurring. Id. The exact occurrence or precise injuries need not have been foreseeable. Iannelli, 145 N.H. at 194. Rather, where the defendant's conduct has created an unreasonable risk of criminal misconduct, a duty is owed to those foreseeably endangered. See id.

Thus, if a private investigator or information broker's (hereinafter "investigator" collectively) disclosure of information to a client creates a foreseeable risk of criminal misconduct against the third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm. In determining whether the risk of criminal misconduct is foreseeable to an investigator, we examine two risks of information disclosure implicated by this case: stalking and identity theft.

It is undisputed that stalkers, in seeking to locate and track a victim, sometimes use an investigator to obtain personal information about the victims. See Note, Stalking Humans: Is There A Need For Federalization Of Anti-Stalking Laws In Order To Prevent Recidivism In Stalking?, 50 Syracuse L. Rev. 1067, 1075 (2000) (discussing two high profile California cases where the stalkers used investigators to obtain their victims' home addresses).

Public concern about stalking has compelled all fifty States to pass some form of legislation criminalizing stalking. Approximately one million women and 371,000 men are stalked annually in the United States. P. Tjaden & N. Thoennes, Nat'l Inst. of Justice Ctr. for Disease Control and Prevention, Stalking in America: Findings from the National Violence Against Women Survey, Apr. 1998, at 2. Stalking is a crime that causes serious psychological harm to the victims, and often results in the victim experiencing post-traumatic stress disorder, anxiety, sleeplessness, and sometimes, suicidal ideations. See Mullen & Pathe, Stalking, 29 Crime & Just. 273, 296-97 (2002). Not only is stalking itself a crime, but it can lead to more violent crimes, including assault, rape or homicide.

See, e.g., Brunner v. State, 683 So. 2d 1129, 1130 (Fla. Dist. Ct. App. 1996); People v. Sowewimo, 657 N.E.2d 1047, 1049 (Ill. App. Ct. 1995); Com. v. Cruz, 675 N.E.2d 764, 765 (Mass. 1997).

Identity theft, i.e., the use of one person's identity by another, is an increasingly common risk associated with the disclosure of personal information, such as a SSN. Komuves, We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. Marshall J. Computer & Info. L. 529, 534 (1998). A person's SSN has attained the status of a quasi-universal personal identification number. Id. at 531-32. At the same time, however, a person's privacy interest in his or her SSN is recognized by state and federal statutes, including RSA 260:14, IV-a (Supp. 2002) which prohibits the release of SSNs contained within drivers' license records. See also Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801-6809 (2000); Privacy Act of 1974, 5 U.S.C. § 552a (2000). "[A]rmed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck." Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993).

Like the consequences of stalking, the consequences of identity theft can be severe. The best estimates place the number of victims in excess of 100,000 per year and the dollar loss in excess of $2 billion per year. LoPucki, Human Identification Theory and the Identity Theft Problem, 80 Tex. L. Rev. 89, 89 (2001). Victims of identity theft risk the destruction of their good credit histories. This often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated. Id. at 91.

The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information.

III. Questions 2 and 3

A tort action based upon an intrusion upon seclusion must relate to something secret, secluded or private pertaining to the plaintiff. Fischer v. Hooper, 143 N.H. 585, 590 (1999). Moreover, liability exists only if the defendant's conduct was such that the defendant should have realized that it would be offensive to persons of ordinary sensibilities. Id. "It is only where the intrusion has gone beyond the limits of decency that liability accrues." Hamberger v. Eastman, 106 N.H. 107, 111 (1964) (quotation omitted); see Restatement (Second) of Torts § 652B comment d at 380 (1977).

In addressing whether a person's SSN is something secret, secluded or private, we must determine whether a person has a reasonable expectation of privacy in the number. See Fischer, 143 N.H. at 589-90. SSNs are available in a wide variety of contexts. Bodah v. Lakeville Motor Express Inc., 649 N.W.2d 859, 863 (Minn. Ct. App. 2002). SSNs are used to identify people to track social security benefits, as well as when taxes and credit applications are filed. See Greidinger, 988 F.2d at 1352-53. In fact, "the widespread use of SSNs as universal identifiers in the public and private sectors is one of the most serious manifestations of privacy concerns in the Nation." Id. at 1353 (quotation omitted). As noted above, a person's interest in maintaining the privacy of his or her SSN has been recognized by numerous federal and state statutes. As a result, the entities to which this information is disclosed and their employees are bound by legal, and, perhaps, contractual constraints to hold SSNs in confidence to ensure that they remain private. See Bodah, 649 N.W.2d at 863.

Thus, while a SSN must be disclosed in certain circumstances, a person may reasonably expect that the number will remain private.

Whether the intrusion would be offensive to persons of ordinary sensibilities is ordinarily a question for the fact-finder and only becomes a question of law if reasonable persons can draw only one conclusion from the evidence. See Swarthout v. Mutual Service Life Ins. Co., 632 N.W.2d 741, 745 (Minn. Ct. App. 2001). The evidence underlying the certified question is insufficient to draw any such conclusion here, and we therefore must leave this question to the fact-finder. In making this determination, the fact-finder should consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." Bauer v. Ford Motor Credit Co., 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001). Accordingly, a person whose SSN is obtained by an investigator from a credit reporting agency without the person's knowledge or permission may have a cause of action for intrusion upon seclusion for damages caused by the sale of the SSN, but must prove that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.

We next address whether a person has a cause of action for intrusion upon seclusion where an investigator obtains the person's work address by using a pretextual phone call. We must first establish whether a work address is something secret, secluded or private about the plaintiff. See Fischer, 143 N.H. at 590.

In most cases, a person works in a public place. "On the public street, or in any other public place, [a person] has no legal right to be alone." W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 855 (5th ed. 1984).

A person's employment, where he lives, and where he works are exposures which we all must suffer. We have no reasonable expectation of privacy as to our identity or as to where we live or work. Our commuting to and from where we live and work is not done clandestinely and each place provides a facet of our total identity.
Webb v. City of Shreveport, 371 So. 2d 316, 319 (La. Ct. App. 1979). Thus, where a person's work address is readily observable by members of the public, the address cannot be private and no intrusion upon seclusion action can be maintained.

IV. Question 4
"One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." Restatement (Second) of Torts § 652C at 380. In Hamberger, we noted that the law of invasion of privacy consists of four separate causes of action, including appropriation. Hamberger, 106 N.H. at 110-11. However, we have not had occasion to recognize appropriation as a cause of action within the State. We now hold that New Hampshire recognizes the tort of invasion of privacy by appropriation of an individual's name or likeness, and adopt the Restatement view. "The interest protected by the rule . . . is the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others." Restatement (Second) of Torts § 652C comment a at 381.
Tortious liability for appropriation of a name or likeness is intended to protect the value of an individual's notoriety or skill. Thus, the Restatement notes, in order that there may be liability under the rule stated in this Section, the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness. The misappropriation tort does not protect one's name per se; rather it protects the value associated with that name.
Matthews v. Wozencraft, 15 F.3d 432, 437 (5th Cir. 1994) (citation, brackets and quotation omitted). Appropriation is not actionable if the person's name or likeness is published for "purposes other than taking advantage of [the person's] reputation, prestige or other value" associated with the person. Restatement (Second) of Torts § 652C comment d at 382-83. Thus, appropriation occurs most often when the person's name or likeness is used to advertise the defendant's product or when the defendant impersonates the person for gain. Matthews, 15 F.3d at 437; see Restatement (Second) of Torts § 652C comment b at 381.
An investigator who sells personal information sells the information for the value of the information itself, not to take advantage of the person's reputation or prestige. The investigator does not capitalize upon the goodwill value associated with the information but rather upon the client's willingness to pay for the information. In other words, the benefit derived from the sale in no way relates to the social or commercial standing of the person whose information is sold. Thus, a person whose personal information is sold does not have a cause of action for appropriation against the investigator who sold the information.

V. Question 5
The last issue relates to the construction of the Consumer Protection Act, RSA chapter 358-A. "On questions of statutory interpretation, this court is the final arbiter of the intent of the legislature as expressed in the words of a statute considered as a whole." Franklin Lodge of Elks v. Marcoux, 147 N.H. 95, 96 (2001) (quotation omitted). We begin by considering the plain meaning of the words of the statute. Snow v. American Morgan Horse Assoc., 141 N.H. 467, 471 (1996). In conducting our analysis "we will focus on the statute as a whole, not on isolated words or phrases." Id. "[W]e will not consider what the legislature might have said or add words that the legislature did not include." Minuteman, LLC v. Microsoft Corp., 147 N.H. 634, 636 (2002) (quotation omitted).
RSA 358-A:2 (1995) states, in pertinent part:
It shall be unlawful for any person to use . . . any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such . . . unfair or deceptive act or practice shall include, but is not limited to, the following:
. . .
III. Causing likelihood of confusion or of misunderstanding as to affiliation, connection or association with . . . another.
Pretext phone calling has been described as the use of deception and trickery to obtain a person's private information for resale to others. See Com. v. Source One Associates, Inc., 763 N.E.2d 42, 47-48 n.8 (Mass. 2002). The target of the phone call is deceived into believing that the caller is affiliated with a reliable entity who has a legitimate purpose in requesting the information. RSA 358-A:2, III explicitly prohibits this conduct. The pretext clearly creates a misunderstanding as to the investigator's affiliation.
The defendant argues that our holding in Snow bars recovery in cases such as this because an investigator who makes a pretextual phone call to obtain information for sale does not conduct any "trade" or "commerce" with the person deceived by the phone call. The Consumer Protection Act defines "trade" and "commerce" as including "the

advertising, offering for sale, sale, or distribution of any services and any property . . . ." RSA 358-A:1, II. There is no language in the Act that would restrict the definition of "trade" and "commerce" to that affecting the party deceived by the prohibited conduct. In fact, the Act explicitly includes "trade or commerce directly or indirectly affecting the people of this state." Id. (emphasis added). In Snow, we held that the registering of foals, alone, was not a transaction involving trade or commerce. Snow, 141 N.H. at 471. Such is not the case here. Here, the investigator used the pretext phone call to complete the sale of information to a client. Thus, the investigator's pretextual phone call occurred in the conduct of trade or commerce within the State.

The defendant argues that a person deceived by a pretextual phone call lacks standing to maintain a private cause of action under RSA chapter 358-A because only a buyer or seller in privity with the defendant may recover under the statute. We disagree. According to the statute, "[a]ny person injured by another's use of any method, act or practice declared unlawful under this chapter may bring an action for damages . . . ." RSA 358-A:10 (emphasis added). The statute defines who may bring a private action broadly, Milford Lumber Co. v. RCB Realty, 147 N.H. 15, 17 (2001), and by its plain meaning does not limit the class of persons who have standing to those in privity with the defendant. We find support for this conclusion in the Massachusetts Consumer Protection Act, which is similar in many respects to the New Hampshire statute. See Milford Lumber Co., 147 N.H. at 18; see also Mass. Gen. Laws ch. 93A (1997). When the Massachusetts Consumer Protection Act was amended in 1979, section 9 was changed to permit "any person" (other than commercial entities covered under a separate section) to recover for damages, which "substantially broadened the class of persons who could maintain actions under [the statute]." Van Dyke v. St. Paul Fire and Marine Ins. Co., 448 N.E.2d 357, 360 (Mass. 1983). Consequently, Massachusetts courts have permitted third parties who were not in privity with the defendant to recover for damages caused by the defendant's violation of the statute. Maillet v. ATF-Davidson Co., Inc., 552 N.E.2d 95, 99 (Mass. 1990); see also Ellis v. Safety Ins. Co., 672 N.E.2d 979, 985-86 n.13 (Mass. App. Ct. 1996) (permitting the housemates of an insurance policyholder to maintain an action claiming racial harassment during an insurance investigation despite lack of privity).

Accordingly, 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 RSA chapter 358-A to the person deceived. Remanded.

NADEAU and DUGGAN, JJ., concurred.

APPENDIX III

Statement by Robert Douglas

Before the
Committee on Banking and Financial Services
United States House of Representatives

Hearing On
The Use Of Deceptive Practices To Gain Access To
Personal Financial Information

July 28, 1998

Introduction

Thank you, Mr. Chairman. My name is Robert Douglas and my firm is Douglas Investigations. My firm provides private investigative services to the Washington, DC legal community. While we specialize in complex criminal defense matters, we also provide general investigative services including traditional areas of civil investigation and information search services. It is my experience with the information broker industry that brings me before you today.

First, Mr. Chairman, let me state that I appreciate the opportunity to appear before you to give my perspective on what I believe to be one of the most significant problems facing our nation today. I want to personally thank you for your willingness and desire to address this serious issue and the time you have invested on this problem. I am aware from both the legislation you have introduced and your public comments that you share my concerns about maintaining citizen's financial privacy. I particularly want to thank your Committee's staff, and specifically David Cohen, for the time they have invested with me discussing this problem.

Mr. Chairman, I also would like to single out for recognition your administrative assistant, Bill Tate, for his assistance

in getting this critical issue before you and the Committee. When I first approached Bill with my concerns about this subject, he immediately recognized this as an issue worthy of you and your Committee's attention and moved quickly to bring it before you. For that I am thankful and I believe the American people will be thankful when they learn the scope and dimensions of the problem we are hear today to discuss.

All across the United States information brokers and private investigators are stealing and selling for profit our fellow citizens personal financial information. The problem is so extensive that no citizen should have confidence that his or her financial holdings are safe.

The types of financial information for sale include: Private bank account numbers and balances; stock, bond and mutual fund holdings including the number of shares held; insurance policy data including the types of insurance maintained and the amount or value of the policy; credit card information including account numbers, size of credit lines, and transaction details including specific purchases.

While the theft and sale of this information is occurring on a daily basis, much of societies focus on privacy as it relates to personal information has been concentrated elsewhere. To date, the majority of public scrutiny has been on issues related to basic data collected via the Internet and the explosion of information that is collected everyday as part of routine commercial transactions.

Issues such as the mass collection of citizens social security numbers, home addresses, phone numbers, and purchasing preferences by retailers have dominated the debate. As part of this debate we routinely hear and read of generic "what ifs..." and concerns that "sometime in the near future" a citizen's most privately held information will be easily obtained by anyone willing to pay for it.

Mr. Chairman, I am here today to tell you that we passed that point long ago and somehow it seems no one noticed.

The Sale of Financial Information
By "Information Brokers"

Currently, thousands of information brokers and private investigators are advertising their ability to locate citizen's personal financial information. The advertisements almost uniformly refer to "bank account searches" and/or "asset investigations". These advertisements can be found in legal and investigative trade journals, general circulation newspapers, the yellow pages, and on the World Wide Web.

The genesis of this specialty niche within the information industry is a growing black market that has developed to sell financial and other forms of personal information. As with most black markets, there needs to be a seller of a commodity that can't be obtained t