

Testimony and Statement for the record of

Raul Ubieta  
Police Major, Economic Crimes Bureau, Miami-Dade Police Department  
Miami, Florida

Hearing on

“Internet Data Brokers and Pretexting: Who has Access to Your Records?”

Before the

Committee on Energy and Commerce  
Subcommittee on Oversight and Investigations  
United States House of Representatives

June 22, 2006

Introduction

Mr. Chairman, ranking member, and members of the Committee, good afternoon and thank you for the opportunity to testify on this important issue before you. I also thank the Committee for their leadership in guarding our privacies. My name is Raul Ubieta and I am a Police Major with the Miami-Dade Police Department in Miami, Florida. I have been in law enforcement for 23 years; 11 of those years have been in conducting, supervising or managing investigations. I am currently in charge of my Department’s Economic Crimes Bureau. My duties include the criminal investigations that inflict serious financial hardship on our community. Typically these crimes involve sophisticated theft schemes that include organized criminal groups that commit mortgage fraud, identity theft, bank fraud, and credit card fraud.

Testimony:

I first became aware of this Committee's work last month, when I was contacted by Mr. Thomas Feddo, Majority Counsel for this committee. We spoke about the existence of Internet Data Brokers and the means in which they obtain their information. More importantly, we spoke about how law enforcement, and in particular, my Department, obtains telephone and subscriber records during the course of an investigation. Mr. Feddo also showed me documentation that a detective from my department had utilized PDJ Services, an online data broker from Texas, to obtain cellular telephone information, several times last year. The usage of that service is not in line with established Departmental practice and is not condoned by the Miami-Dade Police Department. In response to this information, a memorandum was prepared for my Director's signature, reminding our personnel of the proper procedures for obtaining such information. The memorandum also cautioned that the use of confidential information obtained from Internet Data Brokers could place a criminal investigation in jeopardy.

Our position is clear. The Miami-Dade Police Department is governed by Florida State Statutes<sup>1</sup> and internal policies that confer law enforcement the authority to utilize subpoenas to obtain confidential information from the official custodian of records. Information such as subscriber data, customer service records, and incoming and outgoing phone calls from either a traditional landline or a cellular telephone can be obtained through the subpoena process.

---

<sup>1</sup> Florida State Statutes Chapter 27.04 and Chapter 934.23

A typical request for confidential information is handled in the following manner: an investigator obtains a telephone number that is relevant to his/her investigation, that investigator then meets with an Assistant State Attorney to verbally present a synopsis of the case, as well as an explanation as to why the telephone record is essential to the investigation. If the case is approved by the State Attorney's Office, a Subpoena Duces Tecum is prepared by the Assistant State Attorney and provided to the investigator. The investigator then presents the Subpoena to the official custodian of records who is directed to provide the requested information.

The ability of the State Attorney's Office to deny an investigator's request for this information and to ask that additional investigation be conducted before the subpoena is granted creates a system of checks and balances that helps to ensure the integrity of this process. I want to emphasize that our established procedures do not impede our ability to accomplish our job. Even during life-threatening emergencies when cellular or traditional telephone number information must be obtained, the official custodians of records will provide law enforcement with the necessary information and a subpoena or court order will be provided within 48 hours.

Online Data Brokers openly advertise on the internet that they can obtain confidential records. This practice is of concern to the public and law enforcement in many ways.

Information such as social security numbers, banking records and personal financial records can be obtained for as little as \$100 and be used to commit identity theft and schemes to defraud. Not only are these “Internet Data Brokers” a threat to our citizens privacy, but the availability of this information is an officer safety concern.

The ability for criminals to obtain confidential information on an undercover officer and utilize that information to harm the officer or their family poses a serious threat to Law Enforcement. These Internet Data Brokers might state that they are a service to law enforcement, as I have testified today, they are not. There is no compelling law enforcement need to obtain confidential records from Internet Data Brokers.

According to the Federal Trade Commission, in 2005, 9.3 million Americans were victims of identity theft with a loss of approximately \$52.6 billion dollars. Your attention and investigation into the practices by which these “internet data brokers” obtain their information is vital to our citizens’ ability to protect their confidential and personal information. I can attest that the primary source of most criminal fraud cases begins with some type of identity theft. The access to confidential data provided from Internet Data Brokers can easily become a conduit for white collar criminals to further their schemes to defraud.

I thank this distinguished Committee for allowing me to address this important issue. I want to assure you that the Miami-Dade Police Department takes the privacy of our citizens very seriously. Procedures and safeguards are in place to ensure that law enforcement personnel comply with applicable laws regarding private information.