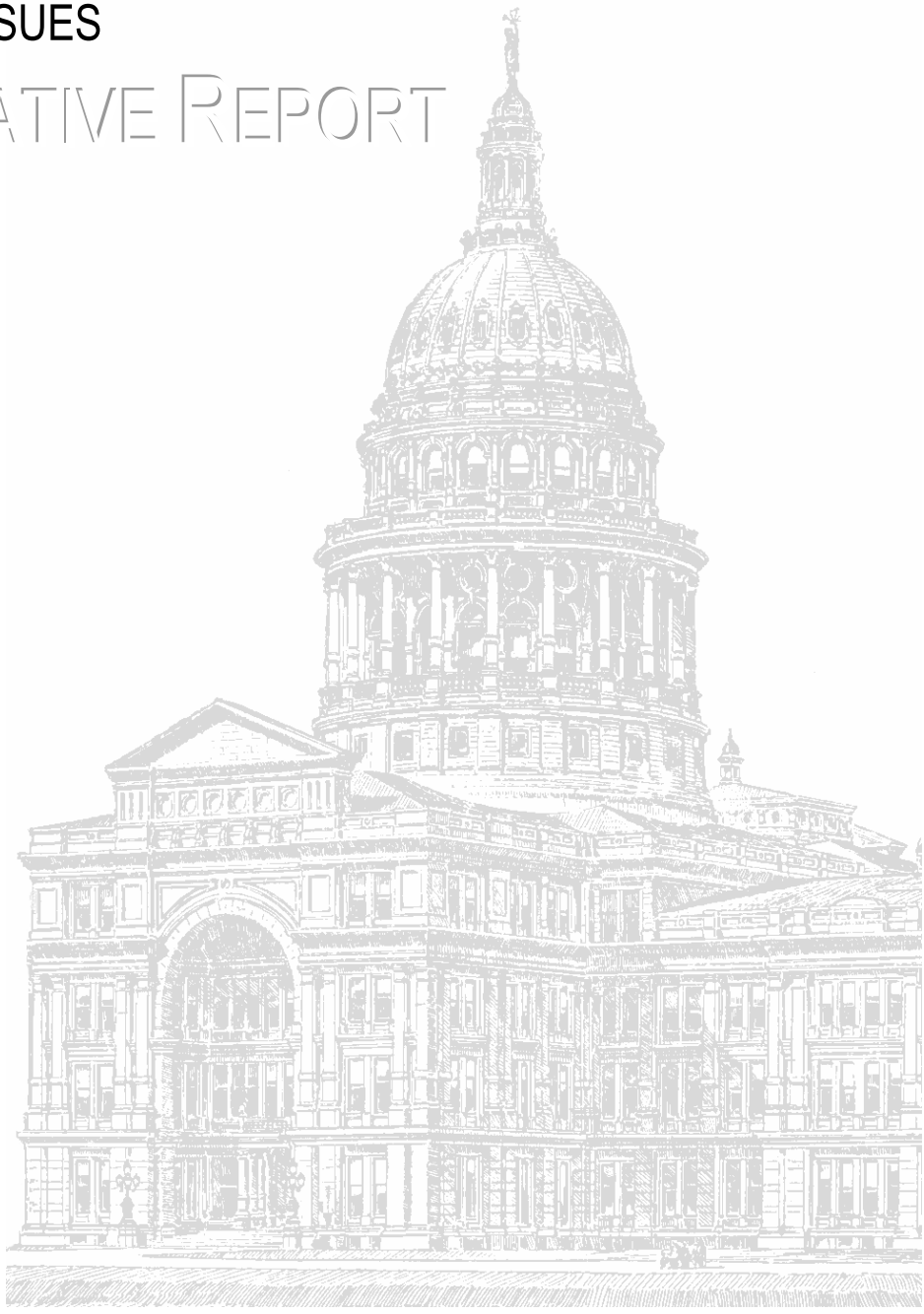
# PAWNSHOP ELECTRONIC DATA TRANSFER REPORT ON RECOMMENDED STANDARDS AND PRIVACY ISSUES

## LEGISLATIVE REPORT



By the

FINANCE COMMISSION OF TEXAS &

THE DEPARTMENT OF INFORMATION RESOURCES

JUNE 30, 2002

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY AND RECOMMENDATIONS

In law enforcement jurisdictions across the state, pawnshops provide information about pawn and purchase transactions to the local police departments and sheriff's offices in myriad ways. Some law enforcement agencies, like Abilene, receive information in the form of paper tickets, and volunteers enter the information into law enforcement computers. Some jurisdictions receive information on paper and use officers to enter the information into local systems, while other jurisdictions receive electronic files specifically formatted for local jurisdictions (often at pawnshop expense). There are also private vendors that collect pawnshop data and, as a private proprietary subscription service, offer jurisdictions the ability to search the data. Regardless of method, all electronic reporting programs to date have been the result of voluntary initiatives between members of the pawnshop industry and law enforcement agencies. These cooperative programs are generally found in the larger Texas cities.

> "In Abilene, eight women known locally as the Granny Squad match about 7,000 pawn shop tickets each month with police reports to help recover stolen merchandise.
>
> In fiscal 2000 alone, the Granny Squad worked more than 1,100 hours and helped return more than $92,000 worth of goods to their rightful owners."[1]

The current environment is characterized by numerous ways of reporting data, disparate computer platforms and software tools used in 146 counties and 318 cities, and 22 different pawnshop software programs running on different platforms. With such an environment, it is essential to create standards for electronically transferring data in an efficient and cost effective manner throughout the state. To this end, House Bill 1763 directed the Finance Commission of Texas and the Department of Information Resources to:

- Create and direct a committee to devise one or more standards for pawnbrokers to electronically provide reportable data to law enforcement
- Consider issues relating to the reporting of the data, including privacy
- Report to the Legislature by June 30, 2002

The Finance Commission of Texas appointed the Consumer Credit Commissioner to chair the committee, while the Department of Information Resources appointed the Program Management Office Director as vice-chair. The chair then solicited five pawnshop industry representatives, five law enforcement agency representatives, three information services vendors, and the Texas Department of Public Safety to be on the committee. The Office of Consumer Credit Commissioner (OCCC) and the Department of Information Resources (DIR) held a series of public hearings around the state to gather information from both the industry and law enforcement. Then in an effort to increase the technical understanding, OCCC and DIR conducted system and operation surveys.

In 2000, 8.8 million pawn transactions were conducted, almost 75 percent occurring in Texas' fifteen (15) largest counties. By comparison, 64 percent of the population resides in those counties.[2] Purchase transactions, where a consumer sells an item to a pawnshop rather than pledging the item as collateral for a loan, are also reported by pawnshops to law enforcement. While the actual volume is unknown, the OCCC survey indicates purchase transactions add ten percent to the total volume. This brings the total transactions to around 10 million reportable transactions statewide. Approximately 75 percent of pledgors redeem their tickets and retrieve the pawned item, therefore, only 25 percent of pawn transactions are potentially linked to property

crimes. Pawn representatives maintain that, historically, less than one-tenth of one percent of all pawn transactions involve stolen property. However, officers of the law articulate that they must deal with 100 percent of the tickets (or electronically transferred ticket data) to find stolen property.

Law enforcement across the state and the country enter information from stolen property reports into the TCIC/NCIC system. To determine whether property is stolen, local law enforcement can send an *inquiry* to the Texas Crime Information Center and the National Crime Information Center (TCIC/NCIC) to find out whether that property is listed in the databank. When law enforcement makes an inquiry of the TCIC/NCIC databank using a particular item's serial number or other identifying information, the computer matches the inquiry information against the stored stolen property reports and returns any matches or *hits*. The TCIC/NCIC systems have recently been updated to modern database technologies, but they are not accessible via the Web nor using Web-based tools. Many law enforcement systems are moving to Web-based standards that allow data transmission and acceptance across platforms and data formats. DPS plans to move the TCIC/NCIC system to a Web-based telecommunications system specifically XML in the future, but no firm timetable for this migration has been established. The need to access TCIC/NCIC in its current environment is a primary driver for the standard recommendation made in this report.

After entering the pawn data in their local agency systems, the law enforcement jurisdiction must use alternative investigative techniques for goods without serial numbers since serial numbers are required for TCIC/NCIC inquiries. Additionally, some law enforcement agencies do not run inquiries on TCIC/NCIC, relying upon serial number matches from contracted systems or from within their internal system. The use of these internal databases and varying controls over the data troubles many pawnbrokers. The pawnbrokers are most concerned by the potential for abuse of the data, whether by the law enforcement agencies or by hackers. Pawnbrokers insist that law enforcement should not have access to any customer information until a link exists to a crime. Law enforcement agencies insist that they already receive customer information across the state and merely desire a change in delivery methods. Law enforcement reports that access to customer information is vital to solving crimes. For example, law enforcement states that individuals with felony property crime backgrounds engaging in an excessive number of transactions should be investigated. One alternative that was suggested is to protect customer information until a customer has engaged in more than a certain number of transactions within a given period of time.

Additionally, pawnbrokers note that even though only a miniscule amount of stolen property is recovered from pawnshops, their industry is heavily regulated. In contrast, other used-goods dealers do not face the same scrutiny, allowing second-hand dealers to traffic in stolen goods without fear of regular, systematic examination or investigation. Law enforcement and pawn industry representatives state that the fencing of stolen goods is occurring more and more frequently through classified ads, at flea markets, or over Internet auction sites, rather than through pawnshops.

> Harris County reported finding and recovering several "Big Bertha" golf clubs stolen from a local retailer through the Internet auction site "eBay."

Clearly, pawnshop computer systems are not a subset of law enforcement systems. Pawnshop systems are created to run the business. Yet the delivery of information from pawnshops to law enforcement remains an important enforcement tool in the resolution of property crimes. The Corpus Christi Police Department reported a 740 percent increase in the recovery of stolen

property in the three years since the department began using electronic pawn ticket data. As described above, there are many areas of conflict around electronically transmitting pawn ticket data, and few issues on which consensus could be reached between the two groups.

This report presents the issues and viewpoints that surround electronic transfer of pawn data and its use within the state's boundaries. As a result, much of this report explores the issues that relate to electronic data reporting; however, recommendations for particular issues, beyond specifying a format, were limited to a few issues. The recommendations are presented here.

| STATUTORILY REQUIRED RECOMMENDATION | |
|---|---|
| **ISSUE** | **RECOMMENDATION** |
| Standard Format(s) for Electronic Reporting | A minimum standard should be mandated with sufficient implementation time to allow smooth uninterrupted transition. An optimum standard should be adopted as a goal for future system improvements to increase the value and use of the data reported. Both standards are detailed in Appendix A. |

| RECOMMENDATIONS IN SUPPORT OF STATUTORILY REQUIRED RECOMMENDATION | |
|---|---|
| **ISSUE** | **RECOMMENDATION** |
| Electronic Reporting System | Any system solution should be contracted out and the contract should be competitively bid. The contract can either be for a vendor to develop a system, or to contract with a vendor to provide a service. The National Association of State Chief Information Officers published a report in 1999, "Toward National Sharing of Governmental Information," that pointed to the use of Extensible Markup Language (XML) as a promising open standard for sharing dynamic structured information as a part of inter-agency or intergovernmental transactions. XML should be considered when looking at system solutions because there are many efforts underway locally, statewide and nationally to use XML for law enforcement-related information exchanges. Any solution will require continued state involvement related to maintaining the standards, as well as coordinating with the Department of Public Safety to ensure interoperability and consistency with other law enforcement-related XML initiatives. |
| Mandated Reporting by Pawnshops | Any pawnshop with a computer system capable of printing pawn tickets should be required to report electronically to law enforcement, however, those not required to electronically report should continue to be required to submit paper copies. |
| System Security and Accountability | If a system is mandated at a regional or statewide level, security of the system should be audited and reviewed regularly by an unbiased external reviewer. |
| Privacy | Consumers should receive disclosure, which could be a part of the Gramm-Leach-Bliley notice, that information about transactions is shared with law enforcement. Information in the system should be protected by the recommendations made for system security and accountability. |

| COMMITTEE CONSENSUS RECOMMENDATIONS BEYOND THE STATUTORILY REQUIRED RECOMMENDATION | |
|---|---|
| **ISSUE** | **RECOMMENDATION** |
| Hold Period | The committee reached a consensus that a procedure for placing items on hold should be included in the CODE OF CRIMINAL PROCEDURE. The procedures should address time limitations. |
| Offense for Falsifying Ownership | The committee reached consensus that establishing an offense for falsifying ownership of property is acceptable. |

# REPORT BACKGROUND

The pawnshop electronic data transfer (EDT) project began in June 2001, when the Texas Legislature passed House Bill 1763 (HB 1763). Section 104 of the bill requires the Finance Commission of Texas and the Department of Information Resources (DIR) to create and direct a committee consisting of representatives from the pawnbroker industry, local and state law enforcement agencies, and developers of software tailored for either law enforcement or pawnshop needs. The committee's task was to devise one or more standard formats for pawnbrokers to electronically provide reportable data to law enforcement agencies and to consider the issues surrounding the use of the format(s) including privacy. HB 1763 set a deadline of June 30, 2002, for the committee to report its findings and recommendations to the Texas Legislature.

The Legislature first considered the topic of pawn EDT during the 75th Session, when HB 2338 and its companion, SB 1274' were discussed. During the 76th Session, HB 2676 and its companion, SB 963, as well as HB 3171, urged the standardization of the EDT process. The 77th Legislature passed HB 1763 requiring the committee be formed and a report written. Appendix B contains a series of planning documents that include the statutory language, the mission statement for the committee, and the project scope statement. Appendix C contains the implementation plan used by the Finance Commission of Texas and the Department of Information Resources to monitor progress.

The committee developed these objectives for the project:

- Define a standard format for electronic data transfer from pawnshops to law enforcement agencies
- Explore the issues, including privacy, relating to the statewide use of the format specified
- Evaluate potential information system solutions to put the standard format into practice

The Finance Commission of Texas is represented on the committee by the Office of Consumer Credit Commissioner (OCCC), the agency that regulates pawnshops in Texas. OCCC and DIR held a series of public hearings throughout the state and conducted a survey of representatives from law enforcement agencies, the pawn industry, and information system providers in order to gain the information necessary to make a recommendation and produce a report.

For a complete description of the project methodology, see Appendix C.

# ELECTRONIC DATA TRANSFER STANDARDS

The purpose of establishing standards is to create a target to work towards, not to enforce compliance on the day that the standards are published. Recognizing the cost of compliance, adoption of standards should include a planned and budgeted transition that takes into account the current environment, priorities, and business directions of industry and government. The most important reason for adopting a standard is the resulting benefit of implementing the standards in the future development of new or enhancements to existing systems.

## Benefits of Standards

The adoption of standards is one component in reducing the total cost of operations for government and industry. Standards are necessary to promote transparent communication across the many systems operating in government and industry; they provide the rules by which information technology products interact with each other and are essential in ensuring that systems can communicate. Standards such as network protocols and interfaces between applications allow systems to share information regardless of hardware and operating system platforms. A standard will provide direction for law enforcement agencies and the pawn industry to manage reporting requirements of high volumes of transactions in an electronic environment. A standard must provide the flexibility necessary to allow both law enforcement agencies and the pawnshops to operate unconstrained.

## Benefits to Law Enforcement Agencies

In the current environment, reporting of pawn ticket information to law enforcement agencies is often a manual, labor-intensive process, subject to a jurisdiction's workload conditions, available resources and priority within the agency. Of the 283 law enforcement agencies responding to a survey conducted by OCCC, less than 25 percent of respondents indicated they are currently capable of receiving information from pawnshops electronically. Agencies currently without EDT capabilities are required to gather paper tickets from pawnshops within their jurisdiction and perform data entry functions to capture the information electronically in order to conduct their investigations. Given the level of effort required to sustain the workload, the level of diligence across jurisdictions varies.

In response to the prevalence of non-automated data reporting, pawnshops and law enforcement have worked together to implement various localized communication systems. In addition, a few third party vendors have developed solutions for data exchange to occur between systems. For a fee, vendors provide law enforcement agencies controlled access to pawnbroker data. The service with the largest market share does not enable the law enforcement agencies to populate their systems with the data, therefore, to conduct property crime investigations, a labor-intensive data entry process must still be maintained. Currently, one such vendor provides this service to 46 law enforcement agencies in Texas, comprising approximately 176 users that are able to conduct electronic inquiries on pawn transactions of approximately 247 pawnshops.

## Benefits to Pawnshops

By administrative rule, pawnshops are required to make pawn ticket information available to a law enforcement agency either electronically or as a paper copy of the pawn ticket. An administrative rule also creates an incentive for the pawn industry to report electronically by allowing a reduction in the length of time a purchased item must be temporarily held before it can be sold.

Implementing a standard transfer method will serve to reduce the reporting burden of pawnshops by eliminating the need to duplicate pawn tickets multiple times for different law enforcement agencies. Additionally, to the extent that more law enforcement agencies seek to obtain pawn ticket data electronically, an EDT solution that automatically adapts to respective data formats of various software programs or a standard data format for transaction reporting will eliminate the need to support multiple electronic transfer solutions.

## Standard Data Elements, Format, Transfer Methods, and Fiscal Issues

The process of defining a standard EDT format for pawnshops to exchange data with law enforcement agencies focused on leveraging existing data elements and format, field specifications and transfer methods currently in use by pawnshops, and data format standards present in the NCIC system. Two standards for data elements were developed, a minimum and optimum format. Each of these is described in Appendix A.

A data transfer standard is intended to solve issues related to electronically reporting data across disparate platforms and systems. Using a standard format, conventional business transactions have been electronically exchanged between governmental agencies, business partners, and other private sector companies for years through an Electronic Data Interchange (EDI) specification. An open exchange of data is a functional prerequisite of EDI, therefore, these standards must remain independent of specific hardware platforms or operating systems. EDI technology, first implemented in the 1960s, relies on dedicated networks and translation software, which is predominately mainframe-centric.

The emerging Internet standard known as Extensible Markup Language, or XML, significantly improves upon the existing EDI standard. It eliminates the requirements to understand each particular program, to prepare systems for data conversion, and to structure an implementation for all users simultaneously to maintain virtual compatibility between senders and receivers. XML is a family of technologies with products available from multiple vendors. XML use does not require one centralized database, as the standards support the exchange of information in a decentralized, distributed environment, as necessary, to multiple law enforcement offices. As government and private industry have sought to eliminate costly private networks and take advantage of the Internet, XML adoption has grown significantly.

Courts, lawyers, and law enforcement agencies locally, statewide, and nationally are implementing XML solutions to improve data exchange. An illustration of the use of XML is the development of a Joint Task Force on Rap Sheet Standardization and the Law Enforcement Intelligence Regional Information Sharing Systems (RISS) initiative, which seeks to create RISS XML specifications to allow dissimilar systems to communicate criminal intelligence information. While law enforcement systems are beginning to employ XML solutions on a large scale, the upgrade to the TCIC/NCIC system will not be completed in the near future. Choosing an Internet based solution like XML

would help reduce the costly conversion issues that could arise from the use of aging data standards.

In examining potential methods for transmitting data electronically, the committee sought to leverage existing capabilities, with specific intent to utilize the Internet as a method for transfer. As described above, less than 25 percent of the 283 law enforcement agencies responding to a survey conducted by OCCC indicated they are currently capable of receiving information from pawnshops electronically. Yet, 80 percent of law enforcement respondents currently have access to the Internet.

The standard data elements, format, and transfer methods recommended in this report are consistent with the requirements of EDI. That is, the standard method for information transferred from pawnshops to law enforcement agencies is based on arranging pawn ticket data in a preset and standardized format as part of the transmission process. The standards can accommodate either fixed- or variable-length format and can be deployed using secure file transfer over the Internet or through e-mail, although the creation of standard data elements, formats, and transport methods could be enhanced using an Internet-based solution, such as XML.

The information in Appendix A is limited to information like field order, field name, field length, and field type. Additionally, a standard for delivery will be required within the development and implementation process. Standards of delivery consist of:

- Encoding methods – such as encryption standards for Internet delivery
- File layout – such as whether the files are delimited or flat fixed length files
- File descriptors – such as whether header records are included or if text qualifiers are included

## Fiscal Issues

To assess the fiscal impact to the pawnshop industry, DIR surveyed pawnshop software vendors to obtain estimates of the cost to implement the minimum data format standard, however, only a few (three of 22) responses were received. Based on the limited feedback received from the software vendor community, it is difficult to extrapolate a total cost, however, the average cost estimated to implement the proposed minimum standard was approximately $1,000 per shop. Additionally, no cost estimates were received from software vendors to determine the implementation cost of the optimum data format. If the number of fields increases, cost could increase as well.

Alternatively, the standard data elements could be implemented using XML, however, the cost of implementing this technology is not included in the estimates provided by the pawnshop software vendors. Many of the XML data element definitions in law enforcement initiatives are currently in draft stage, however, these XML initiatives will bolster the ability in the future to deliver a cost-effective XML solution. A private vendor providing a similar solution, although not deployed in XML, delivers the service for a one time setup fee of $100 per user, thereafter, an annual fee ranging from $600 to $6,000 is charged based upon the number of users. Using these statistics, the cost for this solution is approximately $18,000 in one time charges and $55,000 annually, based upon an average of six to ten investigators per law enforcement agency.

## Issues Surrounding Electronic Exchange of Information

Security and privacy issues must be addressed when implementing any standard for exchanging information electronically. Privacy and confidentiality issues surrounding the transfer of pawnshop customer information to law enforcement are a major concern by the pawn industry. However, regardless of whether the information is electronically or manually entered into law enforcement agencies' systems, safeguards and restrictions regarding privacy of the data must be in place and enforced in order to maintain the public trust.

Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information. Data security is a specific requirement for implementing electronic reporting. While EDI methods ensure secure data transfer through private networks, security over the Internet must be addressed in the deployment of XML. Controls and methods for secure file transfer over the Internet or through secure e-mail must be employed to ensure data in transit is not compromised. To ensure a secure environment, a general system security framework must be deployed that includes authorization and access control that can be implemented through electronic signature and encryption. DIR has promulgated security and web standards for the State of Texas and should be implemented where applicable in any system solution.[3]

## Electronic Data Standards Conclusion

It is evident that some pawnshops are already electronically reporting information to law enforcement across the state, predominately through voluntary partnerships or through a third party vendor whose fee is paid by law enforcement. By setting a standard, the state will provide clear direction for the pawn industry and law enforcement to develop electronic information exchange solutions. Additionally a standard for electronic data reporting will serve to strengthen the marketplace with competitive solutions from third party software vendors. Considering the size and resources available to pawnshops and law enforcement agencies, it is essential to recognize the impact that implementation of standards for data format and transfer will have on both these entities.

# PRIMARY AREAS OF CONCERN

The state of Texas has 1,263 active pawnshop locations. Each of those locations must make available to local law enforcement agencies the information gathered during a pawn loan transaction. Most shops have computerized the pawn process through software packages tailored to the pawn business. Among Texas pawnshops 22 such software systems are in use. Smaller shops still tend to use manual ticket systems, taking down a pledgor's information by hand. Law enforcement agencies use pawn data as a resource to solve property crimes. In some situations, the pawn ticket information can aid in solving violent crimes as well.

Approximately 75 percent of all pawn transactions result in the original owners redeeming their tickets and retrieving their pawned items. Therefore, only 25 percent of the tickets are potentially linked to property crimes. Pawn representatives insist that, historically, less than one-tenth of one percent of all pawn transactions involve stolen property. However, officers of the law articulate that they must access 100 percent of the ticket data to find those transactions to find stolen property.

The *Texas Pawnshop Act* (§371.204) allows officers access to pawnshop records. However, pawn information is often a difficult resource to utilize, due largely to the inherent inefficiency of processing the huge volume of tickets provided to law enforcement as well as certain limitations of the data itself. Streamlining communication and data transfer should provide a means for law enforcement agencies to save time and money in working with pawn data.

§371.204. INSPECTION BY PEACE OFFICER. A pawnbroker shall allow a peace officer to inspect the pawnbroker's books, accounts, papers, correspondence, or other records that relate to the business of the pawnbroker at any reasonable time without judicial writ or other process.

## Lack of Existing Standards and Current Technology

Millions of tickets pour into law enforcement agencies each year. The largest 15 counties account for almost 75 percent of pawn transactions. The Houston Police Department deals with almost 1.4 million reportable transactions from pawnshops in a year, Dallas receives approximately 840,000, and San Antonio receives approximately 1.4 million. Smaller municipalities receive fewer tickets, but also have less staff. For example, a law enforcement representative reported at the Fort Worth hearing that he is responsible for 1,500 tickets a month and uses two people to enter the ticket information.

Receiving the data electronically can dramatically increase the efficiency of law enforcement users. At one of the public hearings, a law enforcement representative estimated that one clerk could enter only 100 transactions per hour—and only 60 transactions per hour if the pawned items have serial numbers. (The law enforcement survey respondents indicated that about 50 percent of the pawn tickets they receive contain serialized merchandise.) With the electronic exchange of data, one law enforcement official indicated that data from 15,000 pawn tickets could be loaded in thirty minutes.

Law enforcement officials state that some jurisdictions use detectives, not clerks, to enter the data entry meaning that if the data was provided electronically, detectives would have significantly more time to investigate crime rather than doing clerical work. Of 105 pawnshops that participated in the OCCC's survey, only five currently provide pawn ticket data electronically to law enforcement.

Electronically exchanging data will benefit hundreds of law enforcement agencies who now accept information on paper that requires manual entry of the data, accompanied by the risk of typing errors. Law enforcement representatives report that often the paper tickets cannot be fully utilized as a resource, because in understaffed departments the tickets listing guns and merchandise with serial numbers are given priority and the remaining tickets are filed away unexamined.

The law enforcement survey, with a statistically reliable response of 72 percent, revealed that while property crimes represent half or more of the crime in 65percent of jurisdictions surveyed, those same departments usually have six or fewer officers to handle property crime investigation.

Even with electronically delivered data, the problem remains of *interdictional* (among jurisdictions) delivery of and access to information. Different agencies tend to have different automation systems. This situation particularly affects the large pawnshop chains that voluntarily create multiple EDT programs to accommodate exchanging data with law enforcement in various jurisdictions throughout Texas. Further, the law enforcement systems are at variance with each other, so that county and city law enforcement agencies have difficulty sharing the information—a practical point not to be overlooked because data sharing is often essential to locating and identifying criminals.

Existing automated systems present another problem as well: lack of existing standards for presentation of data. Not all pawnshop-specific software processes information the same way. According to one law enforcement representative, some software packages have insufficient field space allowed for serial numbers. As a result, pawnshop staff may type in the entire number only to have the system send truncated serial numbers to the law enforcement agency.

However, establishing a standard for data transfer will not help the organizations that lack the necessary technology. OCCC addressed this issue specifically in its survey of pawnshops and law enforcement agencies. The results show that most law enforcement agencies already have sufficient technology resources in place: 80 percent of responding agencies have Internet access and 76 percent of the investigators have e-mail. In contrast, only 32 percent of the independently-owned pawnshops surveyed have Internet access.

## Compatibility with TCIC/NCIC

The FBI's National Crime Information Center (NCIC) is a nationwide criminal justice information system used by local, state, and federal criminal justice agencies to enter or search for stolen property, wanted or missing persons, and other crime data. When a property crime is reported to a police department, for example, that department submits an *entry* to NCIC with essential identifiers for the stolen property. NCIC serves as a national database of stolen property, filled with the entries submitted by law enforcement agencies from all over the country. If a police department should receive information about property with a serial number that may be stolen, the department can send an *inquiry* to the Texas Department of Public Safety (DPS), which then sends the inquiry to NCIC to find out whether that property's serial number is listed in the databank. Making an inquiry of the NCIC databank using a particular item's serial number or other information does not mean the item is then entered into the database as stolen.

The Texas Crime Information Center (TCIC) is a Texas-specific subset of NCIC, containing data only from Texas law enforcement agencies. As the sole administrator of TCIC, only DPS can communicate additions to and searches of the main NCIC database on behalf of the Texas law enforcement agencies that make use of the TCIC services. TCIC processes more than 166,000 transactions per day from local criminal justice agencies. With access to TCIC law enforcement agencies can use pawn ticket serialized data to aid local or regional investigations. More than 1,000 local law enforcement agencies communicate electronically with DPS using longstanding standardized formats.

To make an inquiry of TCIC/NCIC about a particular item, the law enforcement agency needs to provide a serial number and a category code for the item. Assigning a code from a pawned item is not a simple matter, but it can be accommodated in software, if basic property types are captured.

Law enforcement reports that access to TCIC/NCIC is essential for the electronic pawn data because the effort to curb violent crime is augmented by a law enforcement agency receiving data about pawned weapons. The law enforcement agency can then inquire of TCIC/NCIC whether those weapons are in the stolen weapon file. Seventy percent of law enforcement agencies surveyed indicate they run inquiries with TCIC/NCIC, but 75 percent of those must manually enter the information into their automated systems to transmit it to DPS. Therefore, any statewide recommendation must anticipate the ultimate need to create an inquiry within the TCIC/NCIC system.

# PRIVACY

Of all topics related to the establishment of an EDT standard, concerns over privacy issues may be the most controversial. Privacy considerations were raised frequently in the public hearings, usually by representatives of the pawn industry. Brief summaries of each issue are presented below, followed by an analysis of the legal issues involving the privacy and Fourth Amendment issues.

## Privacy Overview

The advent of the digital age may seem to create fears about the privacy rights of individuals; however, concerns about privacy rights are not new. In 5th Century B.C., Greeks recognized the privacy rights of individuals in the Hippocratic Oath**.** The oath provides that what "I may see or hear in the course of treatment or even outside the treatment in regard to the life of men…I will keep to myself."[4]

With respect to privacy rights in the United States, a report issued by Minnesota Attorney General Mike Hatch noted:

> Legal scholars Samuel Warren and Louis Brandeis brought attention to the legal underpinnings of the right to privacy over 100 years ago in their now famous law review article entitled *The Right to Privacy*. In advocating for "the right to be let alone," they reasoned that both the right to liberty and the definition of property can encompass privacy interests and that failure to recognize privacy would mean that "what is whispered in the closet shall be proclaimed from the house-tops." [5]

US Supreme Court Justice Louis Brandeis noted, dissenting in Olmstead v. United States, that:

> The makers of our Constitution…sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred as against the Government, the right to be let alone — the most comprehensive rights of man and the right most valued by civilized men**.**[6]

In America, privacy rights have been granted protection repeatedly by the US Supreme Court by virtue of protections found in the US Constitution. The Court, in fact, has found that privacy interests are rooted in fundamental liberty rights. The Court has recognized certain "zones of privacy" that protect citizens. A marital relationship, for example, lies within such a zone of privacy. The Court has found that Americans have constitutional rights to privacy that protect an individual's freedom of association and the privacy of the home, to name but a few.[7]

The United States Supreme Court has not been the only governmental body to recognize the privacy rights of American citizens. Legislative bodies at the state and federal level have joined suit on such issues, as have state and other federal courts. Although Texas, like many other states, has no comprehensive privacy law, "there are 580 statutes that protect specific personal information in limited circumstances."[8] Even with these protections, a study prepared by DIR acknowledges that the "Public Information Act, the act that governs information management in Texas, does not do enough to protect the personal information of the average citizen in the state of Texas."[9] The study offers several recommendations to ensure that the privacy rights of Texans are protected. One of these states that:

> Agencies must be held accountable for faithfully executing their privacy policies and the law. This includes having strong security measures in place to safeguard private information against unauthorized intrusions and coordinate efforts with authorized third parties to perform unannounced annual checks of portal participating governmental agencies to ensure that privacy policies are being adhered to." [10]

A study prepared for the US Department of Justice revealed that 89 percent of American adults are concerned about the misuse of their personal information.[11] In contrast, the study also revealed that "most people are willing to give up some privacy protection if the trade-off results in a benefit to the public, such as increased public safety, [or] crime prevention"[12]

Interestingly the researchers reported that people have had the most problems with businesses invading their privacy. Of the 38 percent of respondents who claimed to have had their privacy invaded, a full 25 percent reported problems with business entities.[13] It is not surprising, then, that most adults prefer the government maintain the personal information collected for sensitive data collections, such as criminal history record systems.

## Objective

Any EDT recommendation should, to the greatest extent possible, protect the privacy of an individual's personal information, while providing the information necessary to meet the legitimate needs of law enforcement.

## Access to Electronic Pawn Data Systems

Law enforcement and the pawnshop industry believe that access to any information transmitted using an EDT method should be restricted enough to protect the privacy of the consumer. The groups, however, maintain divergent views on how the standard should be defined.

**Pawn Industry:** The industry wants access to electronic pawn data limited not only to police departments, but also to certain individuals within police departments. Representatives also expressed the need for safeguards and standards to ensure that only those with a right to the information can actually access it. Throughout the public hearings, pawn representatives provided several anecdotal examples of inappropriate access to data within existing electronic systems. The story most often told involved a firefighter. The firefighter, from a terminal at the fire station, browsed the city's network and, with no help from anyone in law enforcement, accessed data from pawnshops. The data included customers' names and addresses, along with information about pawned property.

Industry suggested that measures to control information access include password restrictions, audit trails detailing who accessed the information and for what purpose, query history reports, and accountability standards for data misuse.

**Law Enforcement**: Agencies concur that access should be limited to those in a need-to-know capacity, but the individual law enforcement entities want the flexibility to select those individuals within each agency.

Law enforcement agrees that password protections are crucial to a system and that those types of controls are presently in place in most jurisdictions. Police representatives pointed to the confidentiality agreements they must sign to use the TCIC/NCIC as an example of appropriate use restrictions. They added that TCIC/NCIC also requires security and restricted access policies and that extensive privacy protocols already exist, in addition to the statutes guiding the protection of private information. Law enforcement agreed with the pawn industry that there should be audit trails documenting the use of the data and accountability measures associated with its misuse. Law enforcement said that, in most cases, measures are already established to deal with an officer's misuse of information.

## Restricted Use of Information

Pawn industry representatives want certain restrictions placed on law enforcement's use of the pawn information. Law enforcement states that it is accustomed to the existence and use of safeguards and audits to show that information is not misused. Dramatic differences emerged as the two sides weighed potential restrictions. The members of the two groups failed to produce a well-defined, consistent response within their own group. Four major categories of use for the pawn information transmitted electronically were identified.

| Potential Uses of Information |
|---|
| **Property Crimes Only**: Law enforcement could query pawn information for stolen items only. For example, if an individual reported a stereo stolen, law enforcement could search pawn information for the stereo. |
| **Crimes Involving Property:** Law enforcement could query pawnshop data in any situation where property is involved in a crime. For example, in a homicide involving a gun, police could query pawn data for matches to the gun, attempting to identify suspects. |
| **Violent Crimes:** Law enforcement could query pawnshop data when investigating any violent crime. In the case of the recent prison escape by the Texas Seven where the escapees committed a homicide, for example, law enforcement could query pawnshop data by the suspect's name for any information that might be helpful in tracking the criminals. |
| **Any Legitimate Law Enforcement Purpose:** Law enforcement determines how to use the pawnshop data at its disposal to search for any property or suspect in any crime. For example, law enforcement could search pawn data in an attempt to locate individuals with outstanding parking tickets or warrants. Law enforcement mentioned that Son of Sam, a serial killer, was apprehended on a parking ticket. |

The majority of the pawn industry believes that pawn data should be available to law enforcement in cases of violent crime and crimes involving property. Law enforcement representatives agreed that authorized officers should be able to search the pawn data in cases of violent crime and crimes involving property; however, many in law enforcement also stand firmly behind the position that the data should be available to them for any legitimate law enforcement purpose.

**Pawn Industry:** Industry desires to restrict the use of certain information strictly because of the dramatically increased potential for misuse of an electronic system. Representatives contend this shift from the manual system to an electronic system fundamentally changes the privacy considerations due to law enforcement's expanded potential use of the data. The manual ticket system itself presents limits restricting the kinds of searches law enforcement is able to conduct. Industry expressed concern over the data mining capabilities inherent in an electronic database**.** Industry cited the Fourth Amendment (protection from illegal searches and seizures) in their objections to data mining and also expressed concerns about the sensitive nature of the

information. Industry pointed to a *Detroit Free Press* article that illustrated the dangers of a system where personal information is maintained in a database for law enforcement access. The article details abuse of the Law Enforcement Information Network. In one case, a part-time police officer used information he found in the database to find and stalk a female he met on the Internet.[14] Industry also says it doesn't want someone with access to the data to use it for frivolous purposes, like searching for information on a potential son-in-law.

Industry wants access to electronic pawn data restricted to those officers investigating crimes involving property. Industry also expressed a strong desire that no one—regardless of system rights or by virtue of status as a property crimes investigator—be allowed access to consumer information without providing a case number.

**Law Enforcement:** Law enforcement stressed that it simply wants access, via an electronic method, to the information the pawn industry is already required by statute to make available. Because the information is currently provided manually, and in some cases electronically, many in law enforcement fail to understand the restrictions requested by the pawn industry simply because of a change in the delivery method of information.

Law enforcement feels strongly that the data should be available for any legitimate law enforcement purpose. Law enforcement does not want access to the data limited to property crimes investigations. In the public hearings, officers recounted stories of homicides being solved through information contained in a pawn ticket. If the data access had been limited to property crime investigators in these cases, investigators might never have made a connection. The departments feel they should maintain autonomy in assigning access to the pawn data.

Law enforcement feels that its agencies should determine what constitutes a legitimate law enforcement use of information at its disposal, within the limits of the law. One representative with access to pawnshop data through a third-party system utilized that system in an attempt to gather information about the recent Texas Seven escapees. The officer was not in possession of a case number, which is required by the third-party system his agency uses, so he made up a number in order to conduct his search. In the officer's opinion, the pawn data served as a legitimate source from which to gather potential information about the escapees.

## Querying the Data

Agreement exists between the pawn industry and law enforcement that queries of data to locate stolen property would be acceptable. There was little consensus between the two groups relating to other types of queries that should be allowable in an electronic system. The discussions focused on three issues related to data queries: the item information, the pledgor information, and the financial details of the transaction.

### ISSUE 1: ITEM INFORMATION

**Pawn Industry:** Industry representatives expressed concerns about privacy and cited potential Fourth Amendment violations for queries of anything other than property information. They object to any

| Item Description: | |
|---|---|

database queries other than those that return property items. This restriction limits police queries to serial number, description, and other similar fields related to the pledged merchandise.

**Law Enforcement:** There was general consensus among law enforcement that searches for items utilizing serial numbers alone have very limited success, as is done within TCIC/NCIC. Several different law enforcement representatives said that only about 10 percent of the general population records serial numbers.

In addition, pawnshops deal in a high percentage of property that have no serial numbers at all. In the survey conducted for this report, 34 percent of law enforcement jurisdictions said that over 50 percent of the pawnshop data they receive involves non-serialized transaction data. Because so few people can provide serial numbers for their stolen property, and because so many pawn transactions involve property with no serial number at all, police feel their effectiveness in finding the property is severely hampered by queries limited to serial numbers.

### ISSUE 2: PLEDGOR INFORMATION

**Pawn Industry:** Again citing potential Fourth Amendment violations, pawnbrokers strongly oppose queries that produce a pawn customer's information as shown in the accompanying table. Pawn representatives do not want law enforcement to have access to consumer information at all unless a case number is associated with the item search. They object to utilizing a database of their customers as a "black book of likely offenders" to produce frequent pledgor lists and the like and feel that name queries equate to such an act.

| | | | |
|---|---|---|---|
| **Pledgor's Name** (Last Name First) | | | |
| **Pledgor's Address** (Residence) | City | State | Zip |
| **Identification Type and Number** | Height | Sex | DOB |

**Law Enforcement:** Although not unanimous, the general feeling among law enforcement agencies is that the pawn data is a tool for agency use and that departments should be able to perform queries as they see fit. They have an almost universal desire to be able to query the data based on a suspect's name and don't feel that such queries constitute invasion of privacy. One officer stated ardently that if a crime occurred in a given area and he could identify known offenders in the same area, he should be able to enter the names to see if they pawned any items matching the stolen property.

### ISSUE 3: FINANCIAL INFORMATION

**Pawn Industry:** Representatives also say that a customer's financial information, as detailed at right, should not be made available to law enforcement simply because the customer used collateral to secure a loan.

| | |
|---|---|
| **AMOUNT FINANCED**<br>The amount of cash advanced or credit extended to you | **$** |
| **FINANCE CHARGE**<br>The dollar amount the credit will cost you | **$** |
| **TOTAL OF PAYMENTS**<br>Amount required to redeem pledged good on data due | **$** |
| **ANNUAL PERCENTAGE RATE**<br>The cost of your credit as a yearly rate | **$** |
| **PAYMENT SCHEDULE:** Total of Payments is due on Date Due | |
| **ADDITIONAL CHARGE PAID ON REDEMPTION** | |
| **DATE PAID** | **Amount Paid $** |

**Law Enforcement:** Although not all, many in law enforcement claimed to have no use for the financial data. The law enforcement agencies that use this data, do so by searching for marked variance in the amount advanced between similar items. If a difference exists law enforcement believes that either the pawnshop

employee believes the item is stolen and is not willing to risk as much on the item or that the amount is an indication of desperation by the pledgor to obtain the money needed.

## Profiling

Another area of dissension between the parties is the topic of profiling. The following definition of profiling seems appropriate for the purposes of this report:

> a data surveillance technique which is little-understood and ill-documented, but increasingly used. It is a means of generating suspects or prospects from within a large population, and involves inferring a set of characteristics of a particular class of person from past experience, then searching dataholdings for individuals with a close fit to that set of characteristics. [15]

**Pawn Industry:** Industry decries the use of profiling and expressed great fear that any unrestricted pawn ticket reporting system has the potential to increase use of the tactic. Industry argues that there is no difference between racial profiling and the kind of profiling law enforcement could do if allowed to freely query personal data for individuals.

Pawnbrokers fear law enforcement would utilize the electronic data to produce reports such as frequent pledgor lists. A frequent pledgor report lists individuals with frequent pawns within a specified period of time. Pawnbrokers question who would set the standards, if there were any at all, for inclusion on the list. In other words, might someone be a suspect for pawning 10 items, 20 items, or 100 items? And within what period of time? One pawnbroker offered an example of an incident with which he claimed familiarity. He said police called a shop and wanted to talk to a particular customer. When the customer arrived, three patrol cars pulled up and the officers came in and cornered the customer. The pawn representative said all the customer had done was to make 10 pawn loans in a month with an average of $30. The representative felt they harassed the customer from the store to the parking lot over a $300 loan. Industry representatives are adamantly opposed to any system that would allow profiling of their customers.

**Law Enforcement:** Law enforcement agrees that an officer would quickly overstep a person's rights by profiling based upon group affiliation instead of behavior. Further law enforcement claims that queries for frequent pledgors are a common and legitimate function of their agencies. Law enforcement stated a right, in the quest to locate stolen property, to identify an individual who pawns 10 televisions, still in boxes, in a short period of time. A law enforcement officer added that he does not assume an individual has committed a crime simply because his or her name appears on a list of people who frequently pawn items. The individual may be pawning his own television 10 different times. The officer said that he looks for correlative information—things like item types, descriptions, outstanding warrants, previous history—to determine if an individual should be investigated further.

Racial profiling, the tactic of predicting behavior based on racial and ethnic criteria, is clearly discriminatory and was declared illegal by an act of the 77th Texas Legislature. Racial and ethnic profiling involves predicting the behavior of an individual based upon false assumptions made about the group to which an individual belongs.

Police queries of data submitted by pawnshops involve the actual pawn and purchase transaction information.

The law enforcement survey conducted for this project reveals that even though the vast majority of law enforcement agencies receive no data electronically, 70 percent search for individuals who frequently pawn items.

Law enforcement in Houston successfully placed a

criminal in jail because his frequent pawns caught their attention. Police became suspicious when they noticed, through a manual review of pawn tickets, that the individual continually pawned auto parts. On one particular day the individual brought in an excessive number of a particular item, all still in boxes. Investigators retrieved the individual's personal information, contacted, and questioned him. They found out the individual managed a chain auto parts store. The investigators contacted the home office for the chain and found there were theft problems at the store. Law enforcement through monitoring individuals making frequent pawns solved the case and apprehended the thief.

## Legal Considerations

**Pawn Industry Analysis:** A law firm representing some of the industry members concludes that the existing *Texas Pawnshop Act*, the current rules adopted under the Act, and various proposed amendments requiring electronic transfer of information are unconstitutional to the extent they require pawnbrokers to deliver personal information of customers to law enforcement officials.

The Texas Supreme Court has recognized a citizen's right to privacy. In Billings v Aktinson, a 1973 phone (wire) tapping case, the court noted a protection of: "the right to be free from the unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities. The court in subsequent cases, created "zones of privacy." The court declared that any intrusion must be "reasonably warranted for the achievement of a compelling governmental objective that can be achieved by no less intrusive, more reasonable means."[16]

The pawn industry believes that pawnshop customers have a legitimate expectation of privacy in their personal information when pledging property at a pawnshop. They acknowledge that the state has an interest in preventing dealings in stolen goods, however, they believe that an unbridled electronic transfer of information would fail the strict scrutiny test articulated by the Supreme Court.

The pawn industry feels that allowing law enforcement officials access to customer information without requiring either a warrant based on probable cause or other exigent circumstances results in an unreasonable search. The Texas Court of Criminal Appeals has held that the purpose of the Fourth Amendment right protecting citizens from unreasonable searches is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[17] The court also opined that Article 1, Section 9 of the Texas Constitution provides equal and perhaps more protection than the Fourth Amendment right. If an individual has a reasonable or legitimate expectation of privacy and the actions of a government official have intruded on this expectation, an unreasonable search has taken place. The pawn industry believes that by obtaining personal information on pawnshop customers, the government is engaging in a search under the Fourth Amendment. They urge that pawnshop customers have a subjective expectation of privacy with respect to personal information that society would recognize as reasonable and, thus, any search must be reasonable. They believe that the *Texas Pawnshop Act*, the current rules adopted under the Act, and various proposals requiring the electronic transfer of information do not constitute either an exception to the warrant requirement or a permissible suspicion-less search.

The pawn industry urges that because its customers are not given the opportunity to be heard about whether their information should be made available to government, the electronic transfer,

and therefore disclosure of personal information, violates the customers' rights to due process. Due process, found in the Fourteenth Amendment, protects citizens from being deprived of their rights without opportunity to be heard.[18] Industry reasons that due process requires some notification to consumers before personal information is transferred. Because the law fails to allow customers the opportunity to be heard before police obtain information, law enforcement is given free reign to compile vast amounts of constitutionally protected information without due process of law.

**Government Analysis:** The *Texas Pawnshop Act* has required pawnbrokers to make available to law enforcement certain information obtained in a pawn transaction since its inception. That information includes a description of the collateral being pledged, as well as the identity of the pledgor. While the Fourth Amendment of the United States Constitution provides a general protection for people from unwarranted searches, this protection has limitations.

When a Fourth Amendment analysis is conducted, one of the major issues centers around the level of regulation of the industry. The pawnshop industry recognizes that it is a highly regulated industry. The state, as a general rule, is permitted to conduct warrantless searches of closely regulated businesses. The rationale is that certain businesses have such a history of extensive government regulation that a person who voluntarily chooses to engage in such a pervasively regulated business does so knowing that business records and reports will be subject to searches and inspections, even without a warrant.[19]

The Court of Criminal Appeals of Texas, in Kipperman vs. the State of Texas, mentioned that:

> beginning in 1874, pawnbrokers have been required by statute to register their transactions in a "book or registry" to be "kept open for inspection"…The details of the transactions to be recorded in the book and on the pawn ticket have long been regulated. [20]

In view of Kipperman, and clearly after more than 100 years of regulation in Texas, it can be stated fairly that pawnshops have long been the subject of close governmental supervision.[21] The pawnshop industry is "highly regulated" to prevent the pawnshops from acquiring stolen property.[22] This is a compelling state interest and justifies the level of regulation and exception to the protections of the Fourth Amendment

Limitations to a customer's expectation to privacy may be found in other areas of law as well. When a person conveys information to a third party for use in a business transaction, that person may no longer have a legitimate expectation of privacy.[23] The law has recognized this loss of privacy by consumers who deal with financial institutions, including pawnshops. When a person provides information to a financial institution, the Fourth Amendment does not prohibit the government from obtaining that information. Similarly, a pawnshop customer has no expectation of privacy for the customer's identity or the identity of the collateral pledged.[24]

The Gramm-Leach-Blilely Act, a statute that regulates financial institutions, details additional privacy standards relating to the information financial institutions collect from consumers. Gramm-Leach-Blilely places many restrictions on what institutions may do with the consumer information they collect. The Act also requires financial institutions, in most cases, to provide consumers a disclosure citing the consumer information the financial institution may release, and to whom. It is important to note, however, that the rule associated with Gramm-Leach-Blilely establishes several

exceptions to the disclosure requirements to consumers. In one exception, notification to consumers is not required when the information they submit is going to be furnished for law enforcement or regulatory purposes. Clearly, the electronic transmission of information collected by a pawnshop to law enforcement falls within the framework of this exception.

Also, these kinds of privacy debates "should properly focus on the use of information beyond the legitimate purposes for which it was initially disclosed—the so-called secondary use of information."[25] Included among the purposes of the *Texas Pawnshop Act* are the following charges:

- Prevent fraud, unfair practices, discrimination, imposition, and abuse of state residents
- Exercise the state's police power to ensure a sound system of making pawn loans and transfers of personal property by and through pawnshops
- Prevent transactions in stolen property and other unlawful property transactions by licensing and regulating pawnbrokers and pawnshop employees
- Assist local governments in the exercise of their police power

In addition, an administrative rule (7 TAC§85.406) requires that pawnshops must make available to law enforcement the information contained on the pawn ticket. The statute and associated rule establish a clear and legitimate purpose for making such information available to law enforcement. If the purpose of making available data contained on the pawn ticket so that law enforcement has access to it, then law enforcement's use of the information falls within the scope of that collection's legitimate use and purpose. No secondary use of the information is contemplated as it relates to the electronic transfer of pawnshop data to law enforcement such as sales of the information to other entities such as third-party telemarketers. The data is confidential by law.[26]

And while the pawn industry expresses concern over the ability of government entities to protect the privacy rights of consumers, one commentator notes:

> When we worry about who might be spying on our private lives, we usually think about the Feds. But the private sector outdoes the government every time. It's Linda Tripp, not the FBI, who's facing charges under Maryland's laws against secret telephone taping. It's our banks, not the IRS, that passed our private financial data to telemarketing firms.[27]

Although the legal arguments dissect the constitutional questions predominating the privacy concern, the ultimate issue boils down to a compelling public policy question–do today's privacy concerns and the use of technology fundamentally change whether or not all of a pledgor's information should be given to law enforcement?

# PERCEIVED BIAS AGAINST PAWNSHOPS AND PAWN CUSTOMERS

At a public hearing, an incident was related where a police officer became suspicious of a particular pledgor because of the frequency with which the pledgor pawned tools. The officer called the pledgor's employer to report that the employee had been pawning tools and find out whether the tools had been stolen from the employer. The pledgor's employer informed the police that the tools did, in fact, belong to the pledgor and that if his employee was pawning all his tools, he must not be paid enough.

Pawn representatives see a marked difference between the state's treatment of their customers as opposed to the customers of other financial institutions. Pawn representatives assert that law enforcement agencies have immediate access to pawn customer data but not to customer data from other types of financial institutions—or other segments of the second-hand sales industry. Other types of businesses offering financial services are not required to regularly report transaction data to law enforcement and the consumers utilizing pawnshops should not be punished as a result.

Longstanding reporting requirements have existed for financial institutions for transactions over a prescribed dollar amount designed to identify tax evaders, money laundering, or drug trafficking. The pawn industry views the practice of providing all pawn transaction data—regardless of dollar amount or any other standard—as less equitable. Further examples of specialized regulatory activity also exist, including the requirement that Texas state money transmitters undergo special regulatory scrutiny designed to locate potentially criminal activity such as money laundering. During a Department of Banking examination, the examiner conducts an analysis of transaction data, searching for trends that might be indicative of criminal activity. Obtaining data about those particular transactions, the examiner may make criminal referrals to the Internal Revenue Service/Criminal Investigation Division, U.S. Customs, or the Texas Attorney General/Financial Crimes Division for further investigation and analysis of the transactions and the parties involved.

Further, some pawn representatives feel that making available to police personal information about pawn customers automatically makes those customers suspects in all property crimes. These representatives object to the idea that obtaining a loan by leaving collateral with the lender, which is not a crime but a viable financial option, is suspicious behavior. As responsible business owners that work with law enforcement to rid communities of crime, pawnbrokers are concerned about the negative perception about their industry and their customers—particularly when that negative perception could result in customer harassment.

At the Fort Worth hearing, a Dallas Police Department representative stated that although the number of stolen items recovered equals a miniscule percentage of all items pawned, the fact is that over 1,000 stolen items are recovered per month in Dallas, equaling over $2 million dollars per year returned to citizens.

Law enforcement responds that the personal information of a majority of adult Texans (but not the financial transactions of those Texans) is already in the DPS Drivers License databank, which is routinely searched by law enforcement authorities for suspects' contact information. The presence of Texans' data in a database used by a law enforcement agency for research is in no way an indictment.

Pawnbrokers assert that only a miniscule amount of stolen items are recovered from pawnshops and yet their industry is heavily regulated. In contrast, other used-goods dealers do not face the same scrutiny, allowing second-hand dealers to traffic in stolen goods without fear of regular, systematic examination or investigation. Pawn industry representatives state that the expensive stolen goods are much more likely to be sold through classified ads, at flea markets, or over Internet auction sites than through pawnshops.

Finally, the industry is opposed to incurring any expense to facilitate EDT, especially if other industries are not required to participate. Representatives point out that pawnshop computer systems are not a subset of law enforcement systems. Large chain stores are already set up on certain software systems to run their businesses and provide executive management with the most comprehensive data. Many of the large chain operations have in fact been successfully putting their systems to use in providing pawn ticket data electronically to law enforcement agencies and in many cases in an impressively sophisticated manner. Changing fields or systems could throw off such established systems, affecting the business processes of the organization and adding even more to the organization's costs.

# FAIRNESS

The pawn industry expresses concerns about the lack of regulation in other segments of the used goods retailing industry and a potential mandate for small, manual-ticket pawnshops to incur the expense of implementing electronic systems

## Lack of Regulation in Other Segments of the Used Goods Retailing Industry

Pawn representatives note that other used goods retailers do not face the same scrutiny that the pawn industry does, allowing second-hand dealers to traffic in stolen goods without fear of regular, systematic examination or investigation. Such retail outlets include flea markets, antique shops, designer clothing consignment stores, jewelry shops, and compact disc (CD) exchanges. Online auction sites also function as second-hand goods retail outlets.

Most used goods dealers are not licensed or regulated. Only retailers that finance the sales of their goods and services, such as furniture stores and home improvement companies, are required to register with the OCCC. In comparison to the licensing process, the registration process is not a rigorous one, consisting only of an initial fee, yearly renewals, and a minimum of paperwork. Further, the agency has significantly less regulatory authority over registered creditors—a marked contrast with the regulation pawnshops experience. Pawnshops are licensed by the OCCC because they make loans to consumers, not because they sell used goods.

The TEXAS PENAL CODE §31.03 requires second-hand dealers to collect and report all the same information that appears on a pawn ticket when the dealers purchase items over $25 in value. The statute specifies the information required in this manner:

> (3) an actor engaged in the business of buying and selling used or secondhand personal property, or lending money on the security of personal property deposited with him, is presumed to know upon receipt by the actor of stolen property (other than a motor vehicle subject to Chapter 501, Transportation Code) that the property has been previously stolen from another if the actor pays for or loans against the property $25 or more (or consideration of equivalent value) and the actor knowingly or recklessly:
>
> > A) fails to record the name, address, and physical description or identification number of the seller or pledgor;
> >
> > (B) fails to record a complete description of the property, including the serial number, if reasonably available, or other identifying characteristics; or
> >
> > (C) fails to obtain a signed warranty from the seller or pledgor that the seller or pledgor has the right to possess the property. It is the express intent of this provision that the presumption arises unless the actor complies with each of the numbered requirements;
>
> (4) for the purposes of Subdivision (3)(A), "identification number" means driver's license number, military identification number, identification certificate, or other official number capable of identifying an individual…

The statute applies to all businesses “engaged in the business of buying and selling used or secondhand personal property.” However, law enforcement representatives report that generally they lack the staff and budget to collect data from used goods dealers. Law enforcement agrees with the pawn industry’s assertion that a very small portion of stolen property is recovered, stating

that second-hand stores, among other outlets, are the more likely vehicles for stolen goods due to the lack of reporting. One police officer noted that although his department knows the most frequently stolen items in his jurisdiction are CDs, the department hasn't been going into the CD exchanges looking for stolen property.

Pawnbrokers assert that a standardized pawn ticket reporting system cannot effectively benefit property crime investigations unless the entire second-hand retailing industry is required to comply with the reporting standards put in place, and compliance is enforced.

## Potential Mandate for All Shops to Adopt Electronic Systems

An inherent aspect of developing standards is determining who must abide by those standards. Small shops with a low volume of business may often continue to use manual multi-copy tickets rather than electronic systems. OCCC estimates that 10-12 percent of Texas pawnshops are still using the manual-ticket systems. Pawn representatives don't feel that manual-ticket shops should be required to purchase computer systems or software to accommodate standards set by the state. Spokespeople for pawnbroker associations predict that ultimately all pawnshop owners will implement computerized systems, particularly when shops are sold or come under new management. Industry supports the concept that any pawnshop currently conducting transactions electronically should provide pawn ticket data electronically. Conversely, manual shops should not be forced to convert to electronic systems.

To address this issue of fairness, the OCCC considered how the as-is concept would apply to other used goods retailers. Because so many used goods dealers use manual-ticket systems, implementing a statewide reporting requirement for flea markets, consignment clothing boutiques, etc. would result in a large volume of paper tickets possibly rivaling the pre-electronic pawn volume. Law enforcement notes that handwritten tickets can be hard to read. Further, a small manual-ticket pawn or second-hand shop may produce very few tickets each month. However, if a large metropolitan jurisdiction contains many small shops then the local law enforcement agency must process a large number of manual tickets. If it is in law enforcement's interest to require all used goods dealers to provide their data electronically, then a mandate to report electronically should include all segments of the used goods industry, including pawnshops.

One alternative to an all-inclusive mandate is to establish a volume threshold based on the number of tickets written. For example, a manual-ticket shop writing more than 100 tickets per month would be required to implement a computerized system and participate in EDT to local law enforcement. The 100-ticket figure was chosen as an example because the OCCC pawnshop survey indicates that the majority of manual-ticket shops write fewer than 100 tickets per month. A generous threshold requires pawnshops to upgrade to an electronic system only if their business increases accordingly as well as permitting the option to maintain current manual systems if business volume is stable.

# SYSTEM OPTIONS

Early in the EDT Project, it became evident that, should this study suggest a standard format for electronically transferring data, the study would also need to explore possible reporting models. The reporting model should meet the needs of both law enforcement and pawnbrokers, as well as protect pledgor information. Members of the pawn industry pointed out that because so many different computer systems are in use, not only within their own group, but among law enforcement as well, that it would be nearly impossible to develop a standard format without standardizing the entire system. How, they asked, would a standard format alone address issues related to all the different computer platforms (PCs, mainframes, Macintoshes, etc.), operating systems (Windows, Apple OS, DOS, Linux, etc.), and software tools (proprietary, commercial, etc.) that would have to be considered? What follows is a description of the four most viable system options considered and an examination of the benefits and disadvantages of each. Because law enforcement would be the primary user of a pawn ticket reporting system, the analysis of the models focuses mainly on the law enforcement perspective.

## The Valuable Role of Technology

In sharp contrast to filling out forms in quadruplicate and maintaining massive files of hard copies, today pawnshops and law enforcement agencies can take advantage of tremendous technological tools. The San Antonio Police Department has developed a sophisticated program that can conduct highly specific and localized searches based upon the stolen property crime patterns experienced within that jurisdiction. The El Paso Police Department realized an 800 percent increase in the recovery of stolen property in the four years since the department began using electronic pawn ticket data. Several Texas police departments, including Dallas and Fort Worth, along with several Texas sheriff's offices such as Tarrant County are utilizing a third party Internet system to meet their EDT needs.

## EDT Experiences in Other States

Several cities in the U.S. and Canada have experimented with pawn EDT development. Minneapolis, Minnesota, Kansas City and St. Louis, Missouri, and Vancouver, British Columbia have successfully implemented systems.

In 1997, the Minneapolis Police Department implemented a pawn ticket reporting system that increased the recovery rates for stolen property. The department's system allows pawnshops to choose the software program to use in the stores; the software requires minimal customization to successfully interface with the departmental system. By 1999, the department had realized a 24 percent reduction in property crimes reported.

In 2001, police departments in Kansas City and St. Louis selected a third party Internet system to address their EDT needs. As a result, these two police departments have decreased administrative cost and improved their investigative abilities by having access to electronic data.

Vancouver police also experienced significant improvements in the stolen property division after adopting an XML pawn ticket reporting system where all pawnshops in the city log transaction data. Because both pawnshops and the department fully utilize the system, the software saved the department hundreds of hours within just the first few months and dramatically increased the

investigators' ability to solve property crimes. For example, the time required to conduct certain research tasks decreased from two weeks to less than sixty seconds, and one investigator estimates that they are solving crimes at three time the previous rate.

A pawn ticket reporting system developed in Florida failed to receive legislative support, but had the potential to reduce hours spent on data entry through automation of data collection and NCIC searches. It was expected to increase the property recovery rate, following the trends set by other pawn ticket reporting systems.

## Ensuring System Success

As part of systems development and prior to selecting any system, the following must be completed:

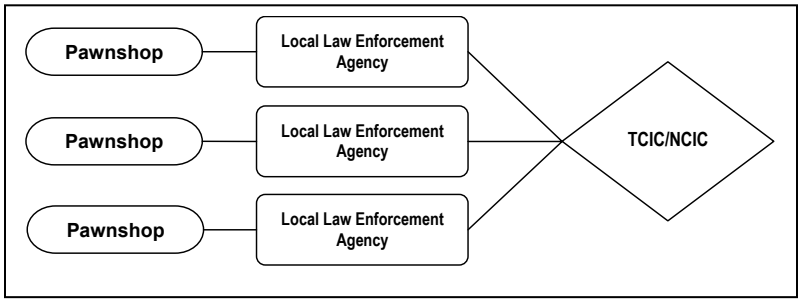
- A formal needs assessment to ensure all user needs are met within the public policy parameters set by the Legislature
- A formal cost benefit analysis to ensure prudent expenditure of funds, and including cost to all parties
- A formal requirements analysis, including exchanging information from pawn shops to law enforcement, and law enforcement to DPS

## Overview of System Options

The committee discussed pawn ticket reporting system models. A description, graphic depiction, and example of each system is presented.

### MODEL 1. DIRECT COMMUNICATION FROM PAWNSHOP TO LOCAL AGENCY

This model most closely mirrors the voluntary one employed in areas where pawnshops and law enforcement first directly exchanged data electronically. Under the model, pawnshops submit data directly to the local law enforcement jurisdiction where the pawnshop operates. The local law enforcement agencies and individual pawnshops work together to develop a method of data transfer that best meets their needs (delivery method, format, and fields). In fact, 56 percent of pawnshops in San Antonio and 96 percent of shops in El Paso voluntarily report to local law enforcement electronically using this model. After receiving the data, local law enforcement agencies manipulate the data to query TCIC/NCIC and to develop and implement other investigative processes. Several major metropolitan areas use this method of data transfer and have developed extensive and highly technical; investigative mechanisms as well. Local law enforcement agencies are responsible for securing the funding necessary to develop the data manipulation capabilities that allow TCIC/NCIC inquiries, as well as the other localized investigative processes.



### SECURITY, ACCOUNTABILITY AND COST

Security would have to be controlled at the local level. A standard, if adopted, should include minimum security and accountability requirements. The cost to implement this model would be low for those local law enforcement agencies already using it. Agencies not using the model already would likely face hardware and system development cost. The link to TCIC/NCIC for agencies with established query protocols would remain unchanged.

**Model 1 in Action**

Each week, Bottle Rocket Pawn creates a disk containing the information from all that week's transactions. Officer Anderson loads the disk into her agency's in-house system. The in-house system manipulates the data, coding it for a TCIC/NCIC batch inquiry and sending the coded information to TCIC/NCIC. The TCIC/NCIC system will report any matches between pawned merchandise and stolen property listed on TCIC/NCIC.

Because the TCIC/NCIC system can only query for items with serial numbers or owner-applied numbers, Officer Anderson's agency has developed specialized investigatory software to supplement the TCIC/NCIC findings. Officer Anderson uses her agency's customized analysis program to complete her search for stolen property among the items contained on the pawn data disk.

### ADVANTAGES

This model allows local control of information sharing, granting a certain amount of flexibility to users in establishing and using their pawn ticket reporting systems. Because the information sharing is local, law enforcement agencies can make decisions for data use on a jurisdiction by jurisdiction basis. Some law enforcement agencies may want to compare the data with other governmental databases. As mentioned earlier, several municipalities have developed sophisticated, investigative methods utilizing the pawn data they receive directly from pawnshops within their jurisdictions. One agency uses pawnshop data in combination with geographic information system (GIS) mapping software to help solve property crimes. This agency might look for a stolen watch using the electronically transferred pawn data in conjunction with GIS mapping software to search for watches pawned within 2 days from when the theft occurred and within a specified area around where the watch was stolen. Information system vendors could continue developing investigative tools and data management solutions.

### DISADVANTAGES

The concept that local law enforcement using this model receive data from only the pawnshops within their jurisdiction is in itself an inherent weakness of this model. A representative of the Tarrant County Sheriff's Office observed that there are 45 to 50 law enforcement agencies within Tarrant county. He went on to say that an investigator in Euless is likely unaware of stolen property in close-by Fort Worth because Fort Worth pawnshops don't report data to Euless. This model fails to solve the communication problem between law enforcement jurisdictions because, under it, information flows only from a pawnshop to the local jurisdiction within which the shop is located. While most jurisdictions would probably check their data against TCIC/NCIC data, it is far less likely that one local law enforcement agency would check for stolen property against other jurisdictions, even if the other jurisdictions were nearby.

Some point out that even with a standard format, law enforcement agencies would still receive data from multiple pawnshops that have different automated systems in different locations. Further the system demands no clear EDT standard of delivery, any adopted option should include a standard of delivery. For example, unless a standard is established, it might be acceptable for one pawnshop to deliver the information to law enforcement on a diskette, while another law enforcement agency might require delivery via an e-mail system. On the other hand, any

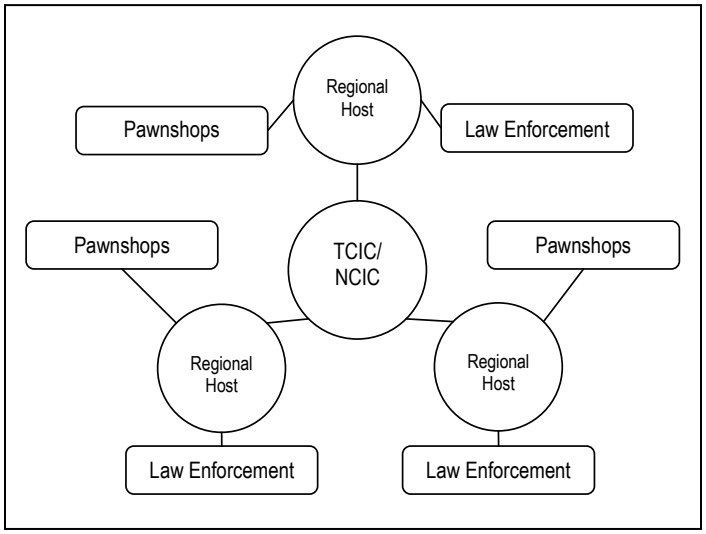
established EDT standard would probably require system changes in some pawnshops and law enforcement agencies.

Chain pawnshops and owners of shops in more than one area would also have to transmit their data to a variety of law enforcement agencies with multiple contact points and, potentially, with varying EDT standards. Without a standard, several chain pawnshops have been voluntarily accommodating multiple law enforcement jurisdictions for years. There is concern that either every pawnshop in the state would have to make accommodations for every law enforcement agency in the state, or vice versa, before a broad-scale utilization of this model could occur.

In one of the public hearings, a pawnshop owner reported that local law enforcement officials without access to electronic data would visit her shop regularly and ask her to search her own systems for data. Law enforcement agencies with so little access or such limited resources would be hard-pressed to participate in electronic data transfer under this model.

### MODEL 2. REGIONAL LAW ENFORCEMENT COMPACTS

In this model, pawnshops would transfer data to a regional data repository maintained by a host law enforcement agency. Local law enforcement agencies would connect to the regional host to search the pawn data from all the jurisdictions within their region. The regional hosts would also process all TCIC/NCIC inquiries for local law enforcement entities. Law enforcement would take the lead in implementing this system, with very little involvement required of state government. It has been reported that the City of Waco operates a kind of regional system, with cooperation of pawnshops and jurisdictions nearby. This model could be compared to the Educational Service Center structure operated through the Texas Education Agency.




**ISSUES WITH SECURITY, ACCOUNTABILITY AND COST**

Simplifying the process greatly when compared to some of the other models, a single system administrator would maintain the physical security of data for each regional host. Because the regional hosts would hold and process all the information, it would be fairly easy to enforce accountability and security standards. Compared to some of the other models, information sharing would be done on a smaller scale, the result of which would be lower cost. Other cost associated with this model include implementation, system development, TCIC/NCIC inquiries, data storage, and reports.

**ADVANTAGES**

Under this model, local jurisdictions would still maintain a great deal of control over information, within the confines of their own region. Each regional system could be tailored to meet the unique demands of its user's needs. Local agencies could share resources and act with flexibility to enhance the system. In fact, other similar kinds of systems exist at local levels and there is the potential to integrate this system with them.

Metropolitan jurisdictions that already have EDT experience potentially could be the regional hosts. The metropolitan jurisdictions might also be able to assist local jurisdictions that currently cannot receive data electronically because they face strained budgets or lack technology expertise. Furthermore, jurisdictions within a given region could search all data within that region. Currently, Bexar County cannot access pawn data from any of the cities within the county. An investigator in Universal City is likely unaware of stolen property in close-by San Antonio because San Antonio pawnshops don't report data to Universal City. Under this model, the investigator in Universal City *could* find property that was stolen in the jurisdiction, but pawned in San Antonio.

**Model 2 in Action**

Wes owns five pawnshops in Round Rock, a suburb of Austin. Once a week, he submits all the pawn data from his five stores to a regional host maintained by the City of Austin. The Austin Regional Host takes the data from Wes, as well as from all the other pawnshops in the region. The computer at the regional host maintains a searchable file of all the information it receives. It also makes a copy of all the information and manipulates the data, coding and transmitting it for a batch TCIC/NCIC inquiry. TCIC/NCIC reports to the regional host any matches between pawned items and the stolen property. The Austin Regional Host then sorts the matches by jurisdiction and sends those sorted matches to the appropriate local law enforcement agency.

The Austin Regional Host also compares the data to stolen property reports from the area, specifically searching any potential stolen property matches among items that don't have unique property numbers to match with.

Under this model, local law enforcement agencies, except for the regional host, would not keep data locally, freeing up computer resources for other purposes. Also, smaller law enforcement agencies might be able to enjoy the benefits of electronic data access at a much more sophisticated level than they might otherwise. Because the regional data hosts would process all TCIC/NCIC inquiries for local law enforcement, the smaller agencies would be able to conduct TCIC/NCIC inquiries, as well as queries of the data held by their regional data host.

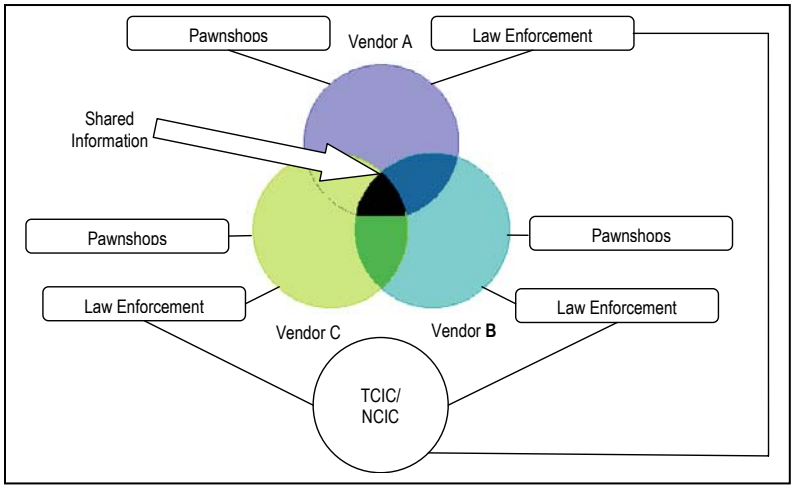
**DISADVANTAGES**

Because local law enforcement agencies would analyze only the data held by their regional host, the ability of widely separated jurisdictions to share information would be severely limited. For example, it is not likely that police in Dallas would be able to search El Paso's data for stolen property.

Potentially, chain pawnshops and owners of shops in more than one area still could be required to report in multiple formats, but to fewer entities than they might in Model 1. A standard data format would significantly mitigate that concern.

Historically, local jurisdictions implementing these kinds of cooperative systems have encountered difficulties due to different local priorities and restrictions on resources. Cooperation would be required among local jurisdictions and inter-local contracts would have to be developed. There may be some local entities less willing to fund such a model in down budget cycles.

## MODEL 3. SINGLE SYSTEM WITH MULTIPLE HOSTS




Similar in many respects to the regional model explored above, this model introduces competition into the EDT process. Private vendors would compete to provide services to law enforcement entities. An oversight body would have to approve that vendors comply with certain minimum standards before they could provide services. Approved vendors would contract with law enforcement agencies and the vendors would collect data from all the pawnshops within a contracting agency's jurisdiction. A pawnshop under the jurisdiction of city law enforcement would only submit data to that city's vendor of choice--the county where the shop resides would not also require the shop to report. A vendor would provide services only to those agencies with whom they have contracts. A law enforcement agency would have access to all of its jurisdiction's pawn information, as well as all the information the selected vendor maintains for its other contracted jurisdictions. If required to meet some specific technology standards, all the vendors potentially could share certain designated information, forming a statewide consolidated data set of specific categories of information (guns, for example, could be designated as a class of item to be shared among all vendors). Any local law enforcement entity could then search the statewide consolidated data through their vendor, regardless of which vendor originally received the data since all vendors would have the consolidated data set. This model most closely resembles the national system operated by the three credit reporting bureaus under the new Fair Credit Reporting Act guidelines that require the sharing of information.

**Model 3 in Action**

The Beaumont Police Department contracts with third-party vendor, DataFinder, to provide pawn data for its jurisdiction. Inez owns a busy pawnshop in Beaumont, so she must send her pawn ticket information to DataFinder. Officer Grace of the Beaumont PD's property crime division uses DataFinder to search for matches between property reported stolen to her division and items pawned. DataFinder provides Officer Grace with a data file to run a batch inquiry through TCIC/NCIC to find matches of property with unique identifying numbers.

At the end of each business day, DataFinder electronically exchanges data with the other approved vendors. The data contains certain essential pieces of information, such as the details of all pawn transactions involving guns. When Officer Grace in Beaumont runs a search for guns, she is accessing the essential data from all the jurisdictions in Texas.

### ISSUES WITH SECURITY, ACCOUNTABILITY AND COST

The data collected by the participating vendors would have to be kept secure by all participating vendors. Accountability issues must be addressed anytime an outside vendor handles sensitive information for government purposes. Clearly, some entity would have to maintain oversight responsibility for the system, adding extra cost. Audits of the system, which would examine issues like data accuracy, the integrity of data security, and system administration, would be required by a statewide administrator.

**ADVANTAGES**

Currently, multiple vendors are marketing solutions to pawnshops and law enforcement and there is no reason to think that these vendors would not be interested in participating in this kind of solution. Under this model, vendors would compete against each other for law enforcement users based upon a given vendor's ability to provide value-added services. Users would not be under a mandate to select any particular vendor. In an effort to gain more business, vendors would likely make enhancements to their own systems, perhaps allowing greater search tools, automatic hold releases, or access to a national database of electronic pawnshop data. In other words, the needs of the market would drive the capabilities of the system. This system would allow and even encourage innovation.

In this model, a vendor would collect all the pawn data from all the jurisdictions with which it contracted, allowing multiple jurisdictions with the same vendor to share information. Additionally, statewide information would be available to users if a minimum standard required vendors to share their data. Classes of items, like guns, could be designated as "must share." The data related to the designated classes would form a statewide, consolidated data set that every vendor would have to make available to all its users. This model also has the potential to allow users a variety of ways to submit data. For example, one vendor could accept data via diskette, while another might only accept data submitted online, assuming standards are adopted to accommodate such flexibility.

With multiple vendors, there is a greater chance that the vendors would tailor their services to local law enforcement needs, allowing local entities to exert some control over the investigative tools and methods. Pawnshops and law enforcement would both be able to choose based on the selection provided and cost charged by different vendors for their services. The nature of the system would also mean there would be more control over data access and use.

**DISADVANTAGES**

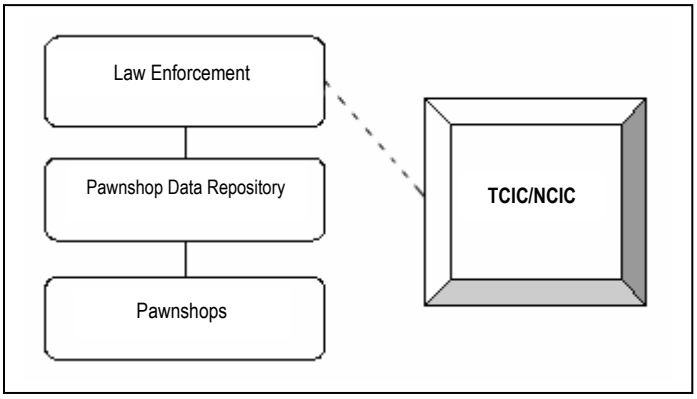
Potentially, chain pawnshops and owners of shops in more than one area still could be required to report in multiple formats, but to fewer entities, than they might in Model 1. A standard data format would mitigate that concern, unless a vendor uses newer technology such as XML. Using XML vendors may be able to receive and manipulate data in multiple formats.

There is no clear solution for overcoming the requirement that law enforcement must conduct queries directly through TCIC/NCIC and not the vendors. Vendors might have to manipulate data and send it back to law enforcement so that the local jurisdictions would be able to run TCIC/NCIC inquiries. This extra step, which has the potential to be costly, would require that law enforcement and the vendors develop standards to facilitate the TCIC/NCIC process. Alternatives could be explored that might allow DPS to accept inquiries from a vendor and deliver responses to local law enforcement agencies. Some smaller agencies with little or no resources may not be able to take advantage of all automated processes, however access to TCIC via single inquiries will always remain an option.

There are some who question the merits of this particular model because they claim the solution is too complex. They believe there are simpler methods to accomplish electronic transfer of pawnshop data. Also, some wondered why vendors would be willing to split the market, especially if some of them would not get enough market share to ensure profitability.

## MODEL 4. CENTRALIZED STATEWIDE SYSTEM—EITHER PUBLICLY OR PRIVATELY MAINTAINED

Under this model, all information would reside with a central repository host. All pawnshops would transmit their data to the host, while all law enforcement entities would conduct inquiries of information through the repository. Several systems electronically transfer pawn data like this, although none on a statewide basis. Florida designed a statewide database of pawn information in a public system, but did not implement it. Several private vendors have also developed databases that maintain pawn data for law enforcement subscribers. A privately contracted model would function very much like the private contracted system that administers the LoneStar Card administered by the Texas Department of Human Services. The advantages and disadvantages of housing the system publicly or privately, through a government agency or through a third-party information system vendor, are explored later in this report.




**Model 4 in Action**

Dave Wasco owns thirty pawnshops throughout Texas. Each week, his company transmits pawn data from all the company's stores to one central repository.

Officer Cavazos works in the pawn detail in a major metropolitan area. Once a week, the central repository sends data from the jurisdiction, formatted for TCIC/NCIC batch inquiries. In addition to TCIC/NCIC match reports received, Officer Cavazos also regularly checks the statewide data in the central repository of pawned items for stolen property.

### SECURITY, ACCOUNTABILITY AND COST

Security in a centralized system is paramount. There would also have to be disaster plans in place to detail actions necessary in an emergency. Accountability would be required of the system administrators, as well as the system users.

### ADVANTAGES

The most important advantage of this model is that it results in a true statewide repository of pawn information that could be queried. TCIC stores statewide information, however the data is limited to certain stolen property. Furthermore, the search capabilities under TCIC/NCIC are very limited because only certain items are listed in the database and all items in it must contain a serial number. Under the centralized statewide model, law enforcement would have access to all pawn data statewide, including items without serial numbers included. Law enforcement in Dallas would be able to search pawn data for stolen property anywhere within the boundaries of Texas. In addition, some believe that because only one host would implement the system, expert knowledge would develop quickly.

Investigative tools could be developed to allow law enforcement the ability to manipulate data. In addition, all pawnshops would transfer data to one host, and all law enforcement would run inquiries through the host, eliminating the concerns both groups have with transmitting/receiving data from multiple sources.

Law enforcement pointed out that a government-housed repository might be able to make TCIC/NCIC inquiries directly to DPS, streamlining the process for local law enforcement statewide.

**DISADVANTAGES**

As with Model 3, a direct link between TCIC/NCIC and the host is absent in this model, therefore alternatives for processing the TCIC/NCIC inquiries would have to be investigated. The private contractor might have to manipulate data and send it back to law enforcement so that the local jurisdictions would be able to run TCIC/NCIC inquiries. This extra step, which has the potential to be costly, would require that law enforcement and the private contractor develop standards to facilitate the TCIC/NCIC process. Some smaller agencies with little or no resources may not be able to conduct the TCIC/NCIC inquiries electronically, though they may still be able to conduct inquiries manually.

.

If a standard format is not developed, then the repository would have to operate the system without a specified format. With a standard, some pawnshops and law enforcement agencies might have to make changes to their own internal systems. Also, unless the standard allowed local jurisdictions to receive extracts of data, the local entities would lose the use of their local and specialized investigative techniques.

Under this model, there would be a sizeable loss in local control. There would be one system with one standard and everyone would have to use it. Because it would be a single system, there would also be very limited room for adaptability.

## State-run versus Third-Party Pawn Ticket Reporting System

The committee spent some time debating the merits of a state-run system versus use of a third-party vendor from private industry. Each approach has its advantages and disadvantages.

| **State-Run System** | **Third-Party System** |
|---|---|
| **Advantages** | **Advantages** |
| • Provides permanent and consistent repository for data<br>• Simplifies implementation and maintenance: one provider, one source, one resource<br>• May help facilitate quick, direct transfer to TCIC/NCIC if managed by a criminal justice agency<br>• Can appropriate funds to contract software developers to provide on-site technical assistance at time of implementation<br>• Allows for system customization to meet law enforcement's crime reporting and analysis needs, taking advantage of interagency confidentiality provisions<br>• Increases drastically the amount and quality of data if use is mandated state-wide, potentially increasing amount of stolen property recovered and number of crimes solved | • Benefits from the market pressure to consistently upgrade and improve services as well as accommodate a wide variety of data file formats<br>• Provides ease of use for pawnbrokers and officers already using third-party systems<br>• Might not require state government funding (but would require local level funding)<br>• Has potentially lower cost, particularly at start-up<br>In a single-vendor system:<br>• Simplifies implementation and maintenance: one provider, one source, one resource<br>In a multiple-vendor system:<br>• Gives law enforcement agencies more options in choosing systems<br>• Opens up room to negotiate price in competitive marketplace |

| State-Run System | Third-Party System |
|---|---|
| **Disadvantages** | **Disadvantages** |
| • Could mandate inflexible requirements rather than creating compatibility with pawnshops' existing systems (particularly during initial implementation)<br>• Would not be motivated by market pressures to place priority on increasing adaptability and features<br>• May present additional cost to taxpayers to develop a system that might already exist<br>• Makes pawn industry uncomfortable due to state's access to data; concern that state government could unilaterally decide to use the data for additional law enforcement purposes<br>• Requires additional employees and related resources to run the system | • May go out of business, placing data access and security at risk (although vendor can place information in a data escrow account for access)<br>• Risks potential lack of compatibility and loss of data integrity when transferring database from one vendor to another, such as prior to the expiration of the contract period<br>• Raises question of data ownership<br>• Restricts access to the data law enforcement wants to conduct their own sophisticated analysis of property crimes<br>• Alternatives for data inquiries to TCIC/NCIC will have to be investigated<br>In a single-vendor system:<br>• Will create a monopoly<br>In a multiple-vendor system:<br>• Can create compatibility conflicts between jurisdictions when accessing each other's data and for pawnshop chain operations transmitting data in various jurisdictions |

## System Options Conclusion

Any system solution should be contracted out and the contract should be competitively bid. The contract can either be for a vendor to develop a system, or to contract with a vendor to provide a service. Prior to developing a request for proposal (RFP) for a system solution, other policy decisions must be made as well such as:

- Determining the oversight and audit responsibilities for the vendor/contractor
- Defining requirements for ensuring that privacy and security are adequately addressed
- Determining how the system development/service provided will be funded (with consideration given to creating an unfunded mandate)
- Determining a transition period for implementation to occur to ensure current information receipt by local law enforcement jurisdictions is not disrupted

It will be necessary to provide funding for the upfront analysis described in the Ensuring System Success section mentioned previously, as well as for the development of the RFP through the selection of a successful bidder. It will be imperative to have a project manager through implementation of a system, and a contract manager to manage the interaction with the successful bidder.

As part of the RFP, vendors will be asked to provide technology solutions that comply with the standards that have been implemented. The National Association of State Chief Information Officers published a report in 1999 "Toward National Sharing of Governmental Information," that

pointed to XML as a promising open standard for sharing dynamic structured information as a part of inter-agency or intergovernmental transactions. Using XML for the electronic data exchange would provide law enforcement agencies throughout the state with the ability to access and share information. As stated earlier, there is a significant effort underway at the national, state, and local levels to exchange criminal justice information using XML.

The state would be required to maintain the data format, and publish the data exchange standards. If this effort evolves into an XML effort, the state would be required to publish the data exchange standard as an XML schema (from the data element standards in this report). All efforts should be coordinated with the DPS, to ensure interoperability and consistency with other law enforcement related XML initiatives.

# FISCAL CONSIDERATIONS

The committee's discussion of fiscal issues concerned three central topics: cost of creating and managing automated systems; sources of funding to cover or defray those cost; and time frames for implementation.

The committee discussed a number of cost and funding factors related to the development and maintenance of automated systems. Pawnbrokers in particular prefer that law enforcement agencies utilize existing software programs tailored to law enforcement's reporting needs, pointing out that creation of an all-new system could delay implementation for years. However, it is difficult to recommend one existing software program that will meet the needs of all agencies *and* pawnshops in all jurisdictions, although there is potential for customizing existing systems to provide the greatest flexibility in data reporting, manipulation, and storage.

Pawnbrokers also object to any suggestion that they or their customers should fund implementation and maintenance of a pawn ticket reporting system run at the state-government level. In fact all taxpayers currently pay for pawn ticket reporting systems at the local level, as individual law enforcement agencies allocate funds for existing systems. Therefore, law enforcement agencies will continue to use taxpayer funds to cover the cost of system implementation and maintenance. During the EDT project hearings, law enforcement officers often made reference to the budgetary constraints under which they work. Law enforcement agencies will need an incentive to adopt any pawn ticket reporting system that might exceed their budgets. These agencies may prefer to continue using the systems they have in place, even inefficient ones.

## Cost

This report is not intended to be a needs assessment, cost benefit analysis, or a customer requirements analysis that would be required before a system for the state could be created or bid. In order to implement and operate a standardized pawn ticket reporting system, a firm budgetary commitment from law enforcement agencies throughout Texas is necessary. Without that commitment, a recommended system will not be feasible. Law enforcement organizations have stated that they would embrace a standardized pawn ticket reporting system if it fits in their budgets, increases their investigatory efficiency, and does not decrease the amount of data they receive through their current systems.

Potential cost of implementation and maintenance of a pawn ticket reporting system may include:

- Hardware (computers, memory chips, etc.)
- Software application maintenance and upgrades
- Technical support
- Internet or intranet connection installation and service

To gain perspective on the total amount required, OCCC researched the pawn ticket reporting system proposed by Florida, a state with a comparably-sized pawn sector. Planners estimated that the overall cost of developing a state-run, statewide pawn

The costs of creating and using an automated pawn ticket reporting system to receive, process, and store pawn data may be offset by these savings factors:

- Decreased payroll cost for data entry clerks
- Increased investigatory efficiency
- Possible increase in number of property crimes solved
- Dramatic decrease in physical storage facilities required for paper pawn tickets

ticket reporting system would cost $1 million.

Clearly law enforcement agencies will have to conduct cost-benefit analyses to determine whether the overall effectiveness and cost-efficiency of their current internal systems justify their continued use. Even departments that already receive and work with some data electronically may face capital expenditures in switching to one of the systems described in this report. For example, the Houston Police Department has a staff of 17 in its pawnshop detail, but only one computer with Internet access—meaning only one detective at a time can use the Internet to conduct investigations or receive information electronically from Internet-based pawn reporting software programs. Adopting a standard pawn ticket reporting system could result in capital expenses for both law enforcement agencies and pawnshops, as existing systems must be adapted to establish compatibility.

## Funding

Other jurisdictions have funded pawn ticket reporting systems by charging pawnbrokers administrative fees in connection with electronic reporting. The Minneapolis Police Department's pawn ticket reporting system is funded by a fee of $2.00 per pawn ticket. Pawnbrokers pass this cost on to their customers. However, no one on the committee believes this is a viable funding option.

Other funding options include

- **Subscriptions paid by law enforcement agencies to a private vendor.** Agencies that currently use private vendors' pawn ticket report systems pay subscription fees to access the pawn ticket information transmitted to the vendors by pawnshops. Bearing cost at the local level generally translates into more control at that level over choice of vendor and in-house systems.
- **Subscriptions paid by law enforcement agencies to a state-run system.** In keeping with the subscription model currently in place for many jurisdictions, agencies could allocate funds for access to the information provided in a state-run information repository.
- **Grant funding.** Funds are available from both governmental and private sources. For example, the U.S. Department of Justice offers funding opportunities to law enforcement agencies looking to implement programs that improve the criminal justice system. However, it is unlikely that grant funding would cover long-term operation cost.
- **Funds appropriated at the state level.** Pawn ticket reporting system cost could shift from the local level (law enforcement agencies) to the state level, possibly allowing for more even distribution of resources and information access throughout the state.

# ISSUES RELATED TO PROPERTY HOLDS

If a law enforcement officer has reason to believe a pawned item is connected with a crime, the officer can place the merchandise on *hold* (have it temporarily taken out of the pawnshop's stock) while the officer investigates its potential connection to a crime. The merchandise remains on-site at the pawnshop but is segregated so that it may not be bought or sold. The length of a hold order varies by jurisdiction. Senate Bill 963, proposed during the 76th Legislature, intended to establish specific state-wide time limits on hold orders. That bill was not passed but in October 2000 the Finance Commission of Texas did adopt administrative rule 7 TAC §85.419 to provide guidelines for the hold order process (detailed later in this section). That rule suggests a period of 60 days for hold orders. Law enforcement representatives and pawnbrokers agree that officers should be granted enough time to adequately conduct investigations; law enforcement prefers an initial hold order of 90 days with the option to renew in 30-day increments.

Law enforcement officers often issue hold orders by phone and follow up later with documentation of the hold. Pawnshop representatives report that they do not always receive the paperwork regarding holds, but strongly prefer to receive documentation to reduce the shops' legal liability. Pawnbrokers expressed frustration about items sometimes being placed on hold for inordinate amounts of time, such as when an investigation is re-assigned to an officer who is not aware of the hold order and does not know to follow up on it. Pawn representatives feel strongly that the officers should initiate and confirm any renewals, as it is not the pawnbrokers' responsibility to follow up on investigations.

Both pawn and law enforcement representatives agree that legislating a uniform system for hold orders would address operational inconsistencies. One pawnbroker advised that each pawnshop should receive hold orders only from officers in the immediate jurisdiction, to ensure consistency in the process. For example, if an officer from Del Rio wanted to place a hold on an item pawned in Lufkin, the Del Rio officer would send the hold order to the Lufkin Police Department for communication to the pawnshop.

## Relevant Statutes and Rules

In response to concerns about the administration of hold orders, OCCC proposed a series of guidelines as 7 TAC §85.419, which was adopted by the Finance Commission of Texas. The rule offers suggested procedures but further legislation may be warranted:

> (a) A law enforcement agency may place a hold order on property.
>
> (b) Suggested guidelines. This section provides suggested guidelines for the placement of hold orders. These suggested guidelines are intended to give pawnshops considerable flexibility to fit individual needs while providing some guidance. Modifications to the guidelines may be made without the loss of protection from any liability defense.
>
> (1) A hold order should be placed in writing by a law enforcement agency. The term of a hold order should not exceed sixty (60) days from the receipt of the written hold order. The law enforcement agency may extend the term of the hold order for additional thirty (30) day increments by notifying the pawnshop in writing. The hold order and all applicable extensions automatically terminate upon expiration.
>
> (2) A hold order or extension should specify:
>
> (A) the name and address of the pawnshop;

(B) the name, title, case number, and phone number of the responsible officer at the law enforcement agency;
(C) a complete description of the property to be held, including model number and serial number, if applicable, and the related pawn or purchase ticket number;
(D) the expiration date of the hold order or the extension; and
(E) the name of the law enforcement agency that prepared the investigative report and the associated number.

(3) A written hold order may be transmitted to the pawnshop by a mutually agreeable method.

(4) Except as provided by this subsection, the property subject to a hold order should not be released, sold, redeemed, or disposed of except under:
(A) release authorization from the official placing the item on hold;
(B) expiration of the hold order and the applicable extensions;
(C) court order, including a search warrant; or
(D) seizure by a law enforcement official.

(5) Property may be released to the custody of a law enforcement agency for use in a criminal investigation if the officer has furnished a written receipt for the property. The release of the property to the custody of the law enforcement agency is not considered to be a waiver or release of the pawnbroker's rights or interest in the property. Upon the earlier of the completion of the criminal investigation or the expiration of the hold order and applicable extensions, the property should be returned to the pawnshop unless a court order provides for other disposition. If other disposition is ordered, the court may order the pledgor or seller to pay restitution in the amount received by the pledgor or seller for the property, plus accrued pawn service charges.

In addition to this rule, the Texas CODE OF CRIMINAL PROCEDURES contains in Chapter 47 the procedures to follow when a hold order is issued by a court rather than by an individual law enforcement officer.

This table provides examples of other states' hold order procedures.

| | Florida | Oklahoma | Missouri |
|---|---|---|---|
| **Length of initial hold order** | 90 days | 30 days | 2 months |
| **Length of renewal** | varies; extension must be court-ordered | 30-day increments (no limit given on number of renewals) | two one-month extensions allowed |
| **Procedure upon expiration** | Pawnbroker sends written notice to officer; if no response by the tenth day after receipt of notice, property reverts to pawnbroker | Unless pawnbroker receives written notice of extension, property automatically reverts to pawnbroker | Pawnbroker sends written notice of expiration to officer; if no response from officer within 10 business days, property reverts to pawnbroker |

Both law enforcement and pawn representatives agree in principle on the value of the hold order in solving property crimes. The process of establishing an automated system may provide an opportunity to concurrently legislate more comprehensive procedures for hold orders.

# ISSUES RELATED TO THE OFFENSE OF FALSIFYING OWNERSHIP

Tangential to the relationship of property crime investigations and pawn data is the subject of penalties for pledgors falsifying ownership of the items they pawn. Some inherent difficulties exist in proving ownership claims: the notoriously high turnover rate in retail means that prosecutors are sometimes not able to locate a particular employee to provide necessary testimony. Also, most consumers fail to record serial numbers or other unique identifiers for their property. However, the statutes that do criminalize the falsification of ownership are valuable tools in the prosecution of property crimes.

At least three states (Colorado, Missouri, and Oklahoma) consider falsification of ownership on a pawn ticket a felony. Oklahoma specifies penalties in its pawnshop-related statutes:

> Any person selling or pledging property to a pawnbroker who uses false or altered identification or a false declaration of ownership as related to the provisions of Section 1515 of this title shall be guilty of a felony, and upon conviction shall be punished by imprisonment in the State Penitentiary not to exceed five (5) years or in the county jail not to exceed one (1) year, or by a fine not to exceed Five Hundred Dollars ($500.00), or by both such imprisonment and fine. (59 O.S. §1512, *Oklahoma Pawnshop Act*)

Texas obliquely addresses falsification of ownership in Chapters 31 and 32 of the TEXAS PENAL CODE. The provisions of §31.03 can apply both to a pawnbroker and a pledgor:

> (b) Appropriation of property is unlawful if:
>
> (1) it is without the owner's effective consent;
>
> (2) the property is stolen and the actor appropriates the property knowing it was stolen by another…
>
> (c) For purposes of Subsection (b)…
>
> (3) an actor engaged in the business of buying and selling used or secondhand personal property, or lending money on the security of personal property deposited with him, is presumed to know upon receipt by the actor of stolen property (other than a motor vehicle subject to Chapter 501, TEXAS TRANSPORTATION CODE) that the property has been previously stolen from another if the actor pays for or loans against the property $25 or more (or consideration of equivalent value) and the actor knowingly or recklessly…
>
> (C) fails to obtain a signed warranty from the seller or pledgor that the seller or pledgor has the right to possess the property. It is the express intent of this provision that the presumption arises unless the actor complies with each of the numbered requirements…

With some exceptions, an offense under §31.03 is generally prosecuted according the stolen property's value, falling into one of these four classes:

- Class C misdemeanor for items valued at less than $50
- Class B misdemeanor for items valued at $50 or more but less than $500
- Class A misdemeanor for items valued at $500 or more but less than $1,500

- A state jail felony for items valued at between $1,500 and $20,000 or—regardless of value—if the property is was obtained through robbery or if the item pawned is a firearm

Another provision that might be applicable is §32.32; an offense under this section is a Class A misdemeanor:

(a) For purposes of this section, "credit" includes:
    (1) a loan of money…
(b) A person commits an offense if he intentionally or knowingly makes a materially false or misleading written statement to obtain property or credit for himself or another…

# END NOTES

1 Texas Comptroller of Public Accounts. Joining the Corps From Fiscal Notes. May, 2002, pg 6.

2 See http://www.window.state.tx.us/ecodata/popdata/cbcopop1990_2000.xls

3 See http://www.dir.state.tx.us/security/policies/tac202.htm and http://www.dir.state.tx.us/standards/srrpub11.htm.

4 Minnesota. Minnesota Attorney General. The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interest in the 21st Century. Minnesota Attorney General's Article, pg 9.

5 Ibid

6 Texas. Department of Information Resources. Privacy Issues Involved in Electronic Government. Austin: Department of Information Resources Report Prepared for the Electronic Government Task Force: Strategic Issues Subcommittee, August 2000, pg 6.

7 Minnesota. Minnesota Attorney General. The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interest in the 21st Century. Minnesota Attorney General's Article, pg 9-10.

8 Texas. Department of Information Resources. Privacy Issues Involved in Electronic Government. Austin: Department of Information Resources Report Prepared for the Electronic Government Task Force: Strategic Issues Subcommittee, August 2000, pg 3.

9 Ibid

10 Ibid, pg 4.

11 Ellard, Timothy D. "Privacy, Technology and Criminal Justice Information: Public Attitudes Toward Uses of Criminal History Information." Search Conference. Washington, D.C. May 31, 2000l, pg 6.

12 Ibid, pg 3.

13 Ibid, pg 7.

14 Elrick, ML. (2001, July 31). Special Report Information Abuse. First of Two Parts. Detroit Free Press, Metro Section, pg 1A.

15 Clarke, Roger. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance." Journal of Law and Information Science 4, 2 (Dec.1993).

16 Billings v. Atkinson, 489 S.W.2d 858, 858 (Tex 1973)

17 Vasquez v. State, 739 S.W.2d 37, 44 (Tex. Crim. App. 1987) (en banc)

18 Pickell v. Brooks, 846 S.W.2d 421, 426 (Tex. Crim. App.—Austin 1992, writ denied).

19 Kipperman v. Texas, 626 S.W.2d 507, 510 (Tex. Crim. App. 1981); S&S Pawnshop Inc. v. City of Delcity, 947 F.2d 432 (10th Cir.1991).

20 Kipperman v. Texas, 626 S.W.2d 507, 510 (Tex. Crim. App. 1981)

21 Kipperman, 626 F.3d at 511

22 TEXAS FINANCE CODE, §371.002 (1, 2, 3, &7).

23 United States v. Miller, 425 U.S. 435, 443 (U.S. 1976); Bayliss v. City of Tulsa, 124 F3d 216 (10th Cir. 1997) cert denied 523 U.S. 1121 (U.S. 1998).

24 Bayliss v. City of Tulsa, 124 F3d 216 (10th Cir. 1997) cert denied 523 U.S. 1121 (U.S. 1998).

25 Minnesota. Minnesota Attorney General. The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interest in the 21st Century. Minnesota Attorney General's Article, pg 27.

26 TEXAS FINANCE CODE, §371.204 and 371.206.

27 Minnesota. Minnesota Attorney General. The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interest in the 21st Century. Minnesota Attorney General's Article, pg 15.