The Bill Blackwood
Law Enforcement Management Institute of Texas

Restricting the Public Information Released by Law Enforcement

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Heath Crossland

Lancaster Police Department
Lancaster, Texas
August 2016

ABSTRACT

The purpose of this paper is to shed light on the release of personal identifying information through government agencies, specifically law enforcement. The Freedom of Information Act of 1967 along with the Texas Public Information Act of 1973 lead to the creation of laws regulating the release of information to the public. When these laws were established, technology was not nearly as advanced as it is today. The lack of updating of these laws leads to the release of personal identifying information of individuals.

In today's modern society, individuals have access to government documents whenever they want. The advent of the internet has created numerous industries that have proven lucrative for those industry pioneers. One industry that has flourished since the advent of the internet are data brokers. These individual companies use technology to obtain large amounts of information off the internet. Data mining is the act of collecting that data. Retailers as well as government agencies use this method to obtain huge amounts of data in order to better their services. They also collect this data through their websites to sell to other businesses for profit.

The problem with this exchange of information is that there is little regulation. Once the requested information is out of the hands of the government agency, there is little regulation of that information. The Business and Commerce Code ("Prohibited use of Crime Victim, 2009) described the sale of crime victim or motor cehicle accident information for the purpose of soliciting business as a class C misdemeanor and the Attorney General's Office needs to pursue charges. Public information released by law

enforcement should be more restrictive. The current laws need revision to protect the individual citizen.

TABLE OF CONTENTS

Page

Abstract

Introduction.....1

Position 2

Counter Position.....5

Recommendation 8

References.....11

INTRODUCTION

Public information released by law enforcement should be more restrictive. Transparency and public information laws allow the release of personal identifying information to the public. That information is available to even more people through the sale of large amounts of public information gathered by private companies. Information is also data. Since the advent of smart phones, many have been introduced to data charges on cellphone bills and understand that customers pay for the data used. Data on smartphones is usually information from the internet and social media that is downloaded, and the cellphone company charges customers on the amount of data downloaded, be it one gigabit or ten gigabits.

The internet is growing at a fast rate. The amount of data available with no restrictions has allowed companies to make millions of dollars collecting that data. The act of collecting data is defined as data mining. Data brokering is selling the data mined in packages to companies or individuals. Data profiles are the packages sold by data brokers. The Federal Trade Commission (FTC) (2016) explained that the very point of data mining is to provide a rational basis upon which to distinguish between individuals. This means creating a data profile based on what a citizen looks at on a particular website or several sites. The FTC (2012) defined data brokers as "Companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for varying purposes, including verifying identification, differentiating records, marketing products, and preventing fraud" (p. 68).

When individuals log into specific accounts on retail sites, their shopping information is tracked by the company to get an idea what the individual is shopping for like coats, hats, blue jeans. The retailers obtain that information and they attach it to the login information, such as an e-mail address or the profile created on that particular retail site. When individuals log into a search engine to check their e-mail or surf the web, search engines like Google, Bing, and Yahoo collect information through a search history and add it to a login profile. This is how advertisements are tailored to interests.

Advertising and marketing companies rely on data mining from search engines and retailers to target their consumers. Retailers and search engines sell the mined data to other companies for profit. Those companies purchase data from all types of sources, including government websites and even credit card companies. The purchasing company separates some data and adds it to other data, creating a more complete data profile.

Open records and transparency laws require government agencies, like law enforcement agencies, to release information to the public when requested. This information may be in hard copy or electronic data. There is no regulation of public information once released. The purchaser of the law enforcement public information can use it and release it how they see fit. Because of this, public information released by law enforcement should be more restrictive.

POSITION

One reason public information released by law enforcement should be more restrictive is that records that are made public may contain personal identifying information of individuals involved in the specific offense. According to Texas Code of

Criminal Procedure Article 15.26 (“Arrest Under Warrant,” 2003), “an arrest warrant and affidavit are public record beginning immediately when the warrant is executed and the Magistrate’s Clerk shall make a copy of the warrant and affidavit available for public inspection during business hours” (para. 1). The Lancaster Police Department (2016), for example, requires the name and date of birth of the defendant on the affidavit for warrant and even more identifying information on the warrant for arrest. Texas Penal Code 32.51 (2013) defines “identifying information” as a person’s personal information, such as name, date of birth, and biometric data. Other identifying information includes sensitive banking information and governmental issued identification numbers.

Another reason public information released by law enforcement should be more restrictive is that the information that is obtained through law enforcement and the courts can be compiled by cooperations to make a profile of individuals and that information can be used to make a profit. Data brokers obtain their information from a large number of resources. These may include government and public records such as court filings (“Data Brokers,” 2016).

Self reported information or individuals providing their own personal information to the industry through online surveys or warranty cards are personal decisions. Using that information to better serve the consumer is the right of the industry. Selling that information within industry circles provides more personal service. It is a perversion of law, however, to apply open records acts to data mining personal information through government agencies. Laws regulating the transparency of government spending and policy such as the FOIA and Texas Public Information Act, are crucial to relationships

between government and the citizens they serve. The goals of both of these acts are for a more open government.

In 1967, “the U.S. government affirmed the right of public access to records other than classified or personal information” (Lordan, 2015, para. 1). A California democrat started a document that would later become the Freedom of Information Act. Newspaper publishers were instrumental in getting the Freedom of Information Act passed during the LBJ Presidency. Within three years of signing the FOIA into law, nearly half of the states had open-records laws. Lordan said that “Today, all states have some form of laws ensuring access to government records” (Lordan, 2015, para 4). Since the passing of the FOIA, government watch dog groups have been able to obtain the important information they were not privileged to in the past. This access gives credibility to the government and insight into possible misconduct.

According to the Austin American-Statesman (2012), Texas created the Texas Public Information Act (TPIA) in 1973. The TPIA is written to favor individuals and organizations requesting government information. The TPIA allows individuals and organizations access to the inner workings of the government, including budgeting processes and lawmaking. The intent of this and other laws like it were not to expose individual citizens to potential criminal activity by releasing their personal information.

Section 552.002 of the Texas Government Code (“Public Information,” 1993) defines “public information” as information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business. The wording of this definition could include individual, personal

identifying information gathered in the daily business of law enforcement. It could also include filing for building permits, garage sale permits, and the like.

Another reason public information released by law enforcement should be more restrictive is that information contained in much of the documents generated by law enforcement is sensitive in nature. The information gathered by law enforcement is usually of criminal activity. The victims and even suspects of this activity can be negativly affected if details of these offenses are made public. Once the information is released to an individual, the information can be distributed how that individual sees fit. Governmental documents along with data profile information including e-commerce and other personal identifying information that is, by law, required to be available to the public can be compiled by any data broker. According to the Federal Trade Commission, “no federal laws require data brokers to maintain the privacy of consumer data unless used for specific purposes” (“Data Brokers,” 2014, para. 7)

COUNTER POSITION

Much of the public believes that the government should be transparent. They feel that the federal and local government should freely provide all information to the public at large. The common thoughts are that the information provided is the right of the people to know. This information is important to having an informed citizenry. The lack of trust of the public and special interest groups in their government has led to the blanket release of information to the public. The laws passed years ago do not take into account current trends in gathering data for official use.

The information regarding government spending and so on is public. There should be organizations that go through these documents and verify that things are true

and correct. However, when it comes to releasing documents with personal identifying information on them, the government should restrict the release only to those with a legal requirement to have said information. An example of this would be an attorney representing a party associated with the report or an insurance company representing a victim of a burglary and the like. Currently, anyone with a report number can obtain a copy of the report. If it is not currently under investigation or in court, it is required by law to be available to the public. In order to make government responsible to the people, they should keep personal identifying information private. Citizens are required to provide so much information to the government on a regular basis that the government should make it difficult for anyone to access it.

The industry of data is highly unregulated. There are currently no federal laws that allow individuals to have access to the information that data brokers have compiled on consumers. Before 1967, the information released to the public was released by those controlling the information. Since the FOIA of 1967, many more documents have been released to the public regarding all kinds of interesting projects the government worked on and the spending on those projects. This information has helped educate the public on the budget of this country and distribution of money to governmental agencies, including contracts awarded and so on.

The FOIA has also been used to uncover scandal within the government. Personal e-mails have been released with details of affairs or misconduct of governmental officials. When the government releases this information, it shows transparency and builds trust that the government is doing the right thing and punishing those who need it by releasing the information that lead to the punishment. When

Edward Snowden was interviewed regarding his release of government information, many thought it was done to get back at the government and he was just releasing secrets. In an interview, Snowden explained, “There are all sorts of documents that would have made a big impact that I didn’t turn over, because harming people isn’t my goal. Transparency is” (Greenwald, MacAskill & Poitras, 2013, para. 51).

A court decision in Dallas, Texas exposed the TPIA as an antique document. This comes because of a request for information from the Dallas mayor’s office where the requestor asked for personal e-mail and text messages from the mayor relating specifically to a topic and not personal affairs or conversations not relating to this topic (Yoakum, 2011). This request was out of the scope of the TPIA at the time. This lead to the court ruling that the information was not required to be released. This became an issue for those requesting information.

Modern technology has caused issue with ownership of the information in question. Supporters of freely released information would say that they have a right to know what conversations were had regarding the topic and if those conversations ultimately influenced the decision that was made on the topic (Yoakum, 2011). The blanket response of open records in this situation could lead to private personal information being released to the public.

State Representative Todd Hunter is pushing a bill in Texas that will clairify the TPIA on the specific topic of technology. This will require government employees with government information to hand over the information to the gorernment body regardless of where that information is stored. Since technology has its place in society, the text

messages and private e-mail that contain government information will be subject to release (Editorial, 2015).

There is not a set standard for accomplishing the task of vetting the information as it relates to government information on private e-mail. Taking private e-mail and sifting through it to find government business will lead to a large surplus of non-governmental information on hand. The surplus is now information gathered through government business and subject to open records after the court inquest is done.

RECOMMENDATION

The government should review and revise the public information laws as they stand. The federal, state, and local government should always be held accountable for the way the tax dollars are spent. The government should always be held to a higher standard than that of private industry. If the government would review and revise the laws as they stand, they will see that the laws are broad in scope, and in a world of instant access, the laws need to be revised to address the access issue.

The government should pass more restrictive public information laws. Less than 15 years ago, there was no such thing as data brokers or data mining, and this is now a multibillion-dollar industry. The industry has clearly outgrown the regulating laws.

Public oversight of governmental decisions and spending will always be a good thing. The passing of this information from the government to the public helps build trust in the government. With so much information available online to the public, the government should not contribute to this data mining industry, it should restrict its diet of public records for the sake of public safety.

The issue of data collection in government agencies is not new to the world. The gathering of census information has been around for quite sometime. Citizens of this country have long been used to filling out forms with line after line of personal information required to obtain whatever service they need from the government. Since data collection and the government go hand in hand, it should not be surprising that as far back as 2003, someone has tried to get the government to see the harm that can come from data collection. The Executive Director of the Electronic Privacy Information Center (EPIC) penned a letter to the House of Representitaves regarding a hearing on "Data Mining: Current Applications and Future Possibilities" (House Government Reform Subcommittee on Technology, 2003).

This letter covered the areas of data collection by the US government. This information was then sold to private companies and then organized and resold to government agencies like law enforcement. EPIC made specific reference to the Privacy Act of 1974 regarding the legality of selling the information and the responsibility of the government, not to sell this information as it violated this Act (House Government Reform Subcommittee on Technology, 2003).

With more restrictive public information laws in place, government can remove itself from the data mining business. This may cut a revenue stream for the government, but the government should not be in business to make money. They are in the business to serve the public and protect each citizen. More restrictive public information laws could also reduce the amount of fraud and identity theft that occurs in the US.

To be truly free in today's world, one needs to be secure in their privacy and know that they are secure in their homes and documents and private affairs. This concept of keeping the government out of private citizens' private lives is a pillar that this country was based on. With the influcence of technology, private citizens have become subject to invasions from not only the government but by private industry as well.

REFERENCES

Arrest Under Warrant, Tex. Code of Crim. Proc., 15.26 (2003).

Data brokers and your privacy. (2016, May). Retreived from https://www.privacyrights.org/content/data-brokers-and-your-privacy

Editorial: Bill clarifies Texas open records laws [Editorial]. (2015, March 1). El Paso Times. Retrieved from http://infoweb.newsbank.com/resources/doc/nb/news/153D0D8F2F54ED98?p=WORLDNEWS

Editorial: Make public record law more open. [Editorial]. (2012, November 27). *Austin American-Statesman.* Retrieved from http://www.statesman.com/news/news/opinion/make-public-record-law-more-open/nTGpD/

Federal Trade Commission Report (2012, March). Protecting consumer privacy in an era of rapid change. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Federal Trade Commission. (2016, January). Big data: A tool for inclusion or exclusion? Retrieved from https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

Fraud, Tex. Penal Code, 32.51 (2013).

Greenwald, G., MacAskill, E. & Poitras, L. (2013, June 11). Edward Snowden: The whistleblower behind the NSA surveillance revelations. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental: Oversight Hearing on Data Mining. (2003, March 23) (Letter from Marc Roternberg, Executive Director, Electronic Privacy Information Center).

Lancaster Police Department. (2016). General orders manual, Directive 7.02.01, Arrest with and with out a warrant, Lancaster, TX: Author.

Lordan, E.J. (2015, January). Freedom of information act goes into effect. *Salem Press Encyclopedia* (Online ed.).

Prohibited use of Crime Victim or Motor Vehicle Accident Information, Tex. Bus. and Com. Code, 504 (2009).

Public Information, Tex. Gov. Code, 552 (1993).

Yoakum, A. J. (2011,January 11). Technical problem: How city of Dallas v. Dallas morning news, LP Exposed a major loophole in the Texas public information act. *St. Mary's Law Journal.* Retrieved from http://www.stmaryslawjournal.org/pdfs/Yoakum.pdf