Delivery Team Report to the Criminal and Juvenile Justice Information Task Force

Commercial Data Mining of Criminal Justice System Records

August 2008

This report was prepared with funding and staff support provided by the CriMNet Program Office, and with staff support from the Department of Corrections, the Department of Administration's Information Policy and Analysis Division and Management Analysis Division, and the Superintendent's Office at the Bureau of Criminal Apprehension.

Contact information for the CriMNet Program Office
Voice: (651) 793-2700
E-mail: crimnet.support@state.mn.us
Fax: (651) 793-2701 Website: http://www.crimnet.state.mn.us
Address: 1430 Maryland Avenue East St. Paul, Minnesota 55106

Other formats
To obtain these materials in an alternative format, — for example, large print or audio file — call voice 651-793-2726 or Minnesota relay, 7-1-1 or 800-627-3529 (voice, TTY ASCII).

Table of Contents

Executive Summary

Minnesota law (Chapter 13) governs the collection, management, and dissemination of government data – in particular, it dictates the rights of individuals who are subjects of the data collected and maintained by government. Extensive procedures outline government responsibilities to inform data subjects and provide them with remedies if information is incorrect or inappropriately disseminated. These procedures, however, only affect government entities.

Criminal justice agencies, like other government entities, collect various pieces of personal data in the regular course of their duties. As agencies discuss sharing of information among criminal justice partners (all government agencies) and the value that represents, they also recognize the impact this sharing may have on the individuals who are the subject of these records. But what has also become more obvious is the impact of government data, created for a specific purpose, being used for decisions in non-governmental contexts – namely housing and employment decisions.

The same technology that provides greater information sharing capabilities for government also enhances the ability of private business to acquire, aggregate, and disseminate data to clients.

During extensive analysis of background checks and expungement of criminal records led by the Criminal and Juvenile Justice Information Policy Group and Task Force in 2006 and 2007, policymakers recognized the need for a greater understanding of businesses that use public data to provide background check services and other activities. The Policy Group noted the importance of understanding both the impact of criminal justice records for state-mandated purposes, as well as records being used outside that context.

This report details the work of a delivery team, appointed by the Criminal and Juvenile Justice Information Task Force, to examine current policy considerations related to non-government use of government data, and to assess how other jurisdictions in the United States have addressed the relationship between government and the businesses who acquire government data.

A number of different approaches have been adopted across the country, from efforts to improve the accuracy of data and require businesses to keep their data current, to applying principles of fair use to the private sector, to allowing data subjects to sue businesses that mine public data, to allowing the industry to regulate itself. Those approaches, and the advantages and disadvantages of each are explored in detail.

The team also discovered a need to educate both data subjects on the remedies available to them and businesses who seem unaware of regulations they may be subject to. For example, subjects have the ability to bring suit against an entity who uses their data, under the federal Fair Credit Reporting Act (FCRA), but they often don't have the means to sue. Further, many business who acquire and provide government data seem unaware they are subject to the FCRA. In other cases, businesses advertise "discreet" background checking services, which indicates no intention of informing data subjects that their information is being used to determine whether they should be granted housing or employment.

The team reviewed each of the approaches identified and informally assessed whether members would recommend certain approaches, recommend the approaches with caution, or not recommend an approach. Though this report does not contain formal recommendations for the Task Force and the

Policy Group, it does provide a broad perspective on the existing practices in an effort to guide policy decisions and perhaps help policymakers create a hybrid solution that addresses the realities for Minnesota.

Overview

During extensive analysis of background checks and expungement of criminal records led by the Criminal and Juvenile Justice Information Policy Group and Task Force in 2006 and 2007, policymakers recognized the need for a greater understanding of businesses (referred to as "data miners") that use public data to provide background check services and other activities. At its June 2007 meeting the Policy Group directed that this delivery team be appointed to research the effects of data mining and make recommendations to the Policy Group about actions that can be taken to address any problems found.

Although the delivery team struggled to reach agreement on defining specific problems and related recommendations, the team did compile significant useful information from which the Policy Group can draw its own conclusions and policy directives. This report identifies various approaches, some of which have been implemented in other jurisdictions that could be used to address data mining.

Whenever people have contact with the criminal justice system, government workers create records. The vast majority of these records are fully accessible to the public. This system of open record-keeping serves public safety interests, as well as society's strong interest in free speech and in a transparent and open justice system. However, in a global and increasingly electronic environment, unintended consequences can result.

Just a decade ago in most jurisdictions, viewing public documents required a visit to the local records clerk who maintained paper files in a cabinet. Today, the electronic nature of many public records allows instantaneous and global dissemination of the smallest record generated by local police, county jails and courthouses. Many commercial data miners[1] collect these electronic government records then sell them for a fee. Litigators use these services to check the backgrounds of jurors, lawyers, and parties. The private sector increasingly uses background checks to reduce risks arising in the employment and housing context. In other words, criminal background checks will be made before someone can be hired or rent a house. Significant public safety benefits are realized when such decisions are based on accurate, up-to-date, and complete government records made readily available by commercial services. The trend toward private background checks is so significant that, as noted by the National Task Force on the Criminal Backgrounding of America, "some law enforcement criminal records repositories now conduct almost as many criminal record checks for civil or noncriminal justice purposes as for criminal purposes."[2]

Once information is given out and no longer in government's control, however, mined records often are practically irretrievable and uncorrectable either by government or by the data subject.[3] Many records, designed for use by police and courts and probation officers in the context of a criminal investigation or court case, now are broadly available for use out-of-context by people unfamiliar with the criminal

[1] There is no agreement about what to call those entities which collect and re-disseminate government data; *data miner* was chosen for the delivery team's work because the words are both descriptive and neutral. Other descriptors include *data aggregator*, *data warehouser*, *data harvester*, and *data broker*.

[2] *Report of the National Task Force on the Criminal Backgrounding of America*, p. 1, viewed online July 3, 2008 at http://www.search.org/files/pdf/ReportofNTFCBA.pdf

[3] The *data subject* is the person about whom information is sought; for example, a job applicant whose background is checked as part of the application process.

justice system. What is understood as a minor matter by those within the criminal justice system may be perceived as deeply significant by those with little exposure to criminal justice records. Further, once controlled by private and commercial interests, the records can take on a quality of permanence never intended by the criminal justice system, possibly resulting in consequences upon the data subject that are out of proportion with the seriousness of the recorded event.

Public policy is evolving to address these new realities. This report provides background about data mining and related issues and provides a review of regulatory approaches taken by various jurisdictions. Additional state safeguards include the following approaches: requiring commercial entities to ensure that the records they sell pertain to the intended subject; requiring data miners to ensure that the data sold is up-to-date; and providing a procedure that gives notice to data subjects and the opportunity to correct errors in data held by private entities.

Delivery Team Formation and Scope

Beginning in June 2007, Minnesota's Criminal and Juvenile Justice Information Policy Group (Policy Group) and its advisory Task Force[4] began to consider the effects of data mining upon people involved with the criminal justice system.[5] At the Policy Group's direction, the Task Force in February 2008 convened a study group to evaluate related issues. This study group (called the Data Mining Delivery Team) defined the scope of the problem broadly; that is, that *the public use of criminal justice data creates adverse impact on data subjects*. The delivery team's discussions focused on public criminal justice record information obtained from government entities and sold by commercial entities. This information includes data about arrests, detention, formal criminal charges and any conviction, dismissal, acquittal or other disposition, sentencing, correctional supervision and release records.

Background

The impact of computer systems on the ability of organizations to retain and process data about individuals was recognized as early as 1973, when a federal advisory committee on automated personal data systems observed that "[t]he computer enables organizations to enlarge their data processing capacity substantially, while greatly facilitating access to recorded data, both within organizations and across boundaries that separate them." In addition, the committee concluded that "[t]he net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems."[6]

Some of the earliest guiding principles used to develop policies governing computerized data are the Fair Information Practice Principles (FIPPs). Five core principles were set forth by the 1973 federal advisory committee (see Appendix A, *Fair Information Practice Principles and the Private Sector*). These FIPPs were adopted in the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13, in the mid-1970s and have been the foundation for legislative decisions about how

[4] The Policy Group and Task Force advise Minnesota's Legislature pursuant to M.S.§299C.65
[5] See *Report of the Background Checks and Expungements Delivery Team*, Minnesota Criminal-Juvenile Justice Task Force and Policy Group, 2006; viewed online July 3, 2008 at http://www.crimnet.state.mn.us/docs/FinalReport.pdf
[6] U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973).

individuals can access and correct data held by Minnesota government agencies. More recently, a federal report on privacy policy stated that FIPPs "provide a straightforward description of the underlying principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated systems."[7] The FIPPs are available to help policymakers design fair and reasonable public policy. The delivery team reviewed the FIPPs and ways they might be applied to commercial data mining activities.

Minnesota's legislature creates comprehensive laws designed to increase the accuracy and accessibility of government-held data. However, the very same data held by commercial data miners is subject to less state regulation. For example, no current state law requires commercial entities to ensure that the records they sell actually pertain to the specific subjects being investigated. Until July 2009 there will be no state requirement that the data sold by commercial data miners be up to date[8]; nor is there a state-enforced procedure in place to allow data subjects to correct errors in data held by private entities (for more information about the 2009 changes, see the following section).

Policy Evolution

Over the past several years, issues created by commercially-mined government data and their impact on individuals have become the subject of increased policy focus both nationally and in Minnesota.

- Nationally, data mining is the focus of research and evaluation that has resulted in reports such as the U.S. Attorney General Report on Criminal History Background Checks;[9] Commercial Use of Criminal Justice Data;[10] the Report of the National Task Force on Privacy, Technology and Criminal Justice Information;[11] and the National Task Force on the Criminal Backgrounding of America.[12]
- **The Federal Fair Credit Reporting Act** (FCRA):[13] FCRA is a federal law that protects consumers by controlling how some personal information is used in the marketplace. Congress passed the first version of this law in 1970 and amended it in both 1996 and 2003. FCRA imposes extensive obligations upon some users of background check data.
- In Minnesota, data mining and related issues have come up in numerous contexts. Legislators have considered several ways their constituents are affected when government-created data are made available for use and re-dissemination by commercial interests. Significant effort has been made in areas involving security breach legislation;[14] use of social security

[7] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, Privacy Policy Development Guide, (Washington, DC: 2005) p. 7-11.
[8] See 2008 Session Laws, Chapter 315, Section 19
[9] *The Attorney General's Report on Criminal History Background Checks*, U.S. Attorney General, 2006.
[10] *Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information*, SEARCH, 2005.
[11] *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, Bureau of Justice Statistics, 2001.
[12] *The National Task Force on the Criminal Backgrounding of America*, SEARCH, 2005.
[13] 15 U.S.C. section 1681 et. seq.
[14] See M.S.§ §325E.61, 325E.64

numbers;[15] background checks, expungement and sealing of criminal records;[16] collateral consequences;[17] and right to access and correct government records[18].

- **2008 Minnesota Data Practices Omnibus Bill:** In 2007 the Minnesota Legislature turned its attention to the data mining industry itself. Legislation authored by Sen. Don Betzold (DFL-Fridley) in Senate File 914 and Rep. Mary Liz Holberg (R-Lakeville) in House File 1306 introduced the idea that state law should require all commercial sellers of government data to refresh their records routinely to ensure that changes at the government source are accurately reflected in commercial databases. Committee consideration led to evaluation of the how the language of the bill might be affected by federal law, particularly FCRA.[19] State laws must be designed so that they avoid preemption by similar federal laws.[20] FCRA protects consumers by controlling how some personal information is used in the marketplace. Congress passed the first version of this law in 1970 and amended it in both 1996 and 2003. Recognizing that not all commercial sellers of government data are regulated by FCRA, the Minnesota Senate Judiciary Committee sought a solution that imposes a data refresh obligation on non-FCRA data sellers while not creating inconsistent requirements for FCRA-regulated entities.

  Senate counsel researched FCRA questions and provided language designed to avoid federal preemption issues. In the 2008 session, the modified language was incorporated into S.F. 3235, the Data Practices Omnibus bill. The modified language allows FCRA-regulated data sellers to follow FCRA and others to be governed by the proposed state law. The Data Practices Conference Committee passed the language with a delayed effective date of July 1, 2009 to allow time for the Data Mining Delivery Team to complete its study and for the Policy Group to develop its recommendations.[21]

The data mining language with its delayed effective date was signed into law by the Gov. Tim Pawlenty on May 15, 2008.

---

[15] See, *e.g.*, M.S.§ 13.355
[16] *Report of the Background Checks and Expungements Delivery Team*, infra.
[17] *Criminal Records and Employment in Minnesota, Report and Recommendations of the 2007 Collateral Sanctions Committee*, Minnesota Sentencing Guidelines, 2008; viewed online July 2, 2008 at http://www.msgc.state.mn.us/projects/collateral_sanctions/Collateral_Sanctions_Report_2008.pdf
[18] See, *e.g.*, M.S.§13.873
[19] 15 U.S.C. section 1681 et. seq.
[20] Preemption is a legal concept that recognizes the supremacy of federal law over state law. Preemption as it relates to FCRA regulation is discussed in detail in Appendix B to this report.
[21] Policy Group recommendations are required by M.S. §299C.65

When FCRA Violations are Invisible to Data Subjects

Gray areas remain despite FCRA's extensive regulation. The Delivery Team considered areas where FCRA might be inadequate to protect data subjects. One example provided to the Delivery Team suggested that a person aggrieved by failure to abide by FCRA may simply have no way to know about the failure and therefore no opportunity to pursue remedies technically available. Rather than devote extensive meeting time to individual testimony, the Delivery Team acknowledged the work done by the Collateral Sanctions Committee[22] as well as numerous examples available from the BCA and other. Such unfairly disadvantaged people have no remedy if they remain in the dark about the employer's background check process.

Further, consider the large number of enterprises that collect criminal records and then make them available through a website for a fee. Some promise "discreet" and "confidential" background checks.[23] If the customers of these websites are using the information for a purpose regulated by FCRA, the business should be complying with the federal law's requirements. However, there is no way for the data subject to know any of these details and, again, FCRA litigation is unlikely.

Data mining can be a very small operation, one which may go unadvised by legal counsel. Web-based background check services can be created by a single entrepreneur with an internet-connected computer, the ability to download public-record government data, the ability to package that data in a way that appeals to online customers, and the capacity to accept online credit card payments. Simply typing the words *background check service* into a Google search will return more than 5 million hits. From the first such screen, consider these few examples:

- ***Datesandlove.com*** promises "a great way to check your new friends, dates, or employees;"
- ***Sittercity.com*** offers a way to check people out for child care, pet care, senior care, home care, and tutoring;
- ***Criminal-records-search.com*** promises that the subject of their background checks will "not know who has requested background checks on them, because it is public records [sic]."[24]

Customers' illegal use of such sites would be, for all practical purposes, invisible. For example, an employer or landlord might use these services to screen applicants, taking no FCRA-mandated actions such as providing notice to the applicant and a copy of the background report to a rejected applicant. Illegal use of this sort is likely to go undetected under current law because FCRA's primary enforcement mechanism requires victims of wrongdoing to hire a lawyer to file a federal lawsuit. It is possible that federal law creates a hurdle too high for individuals who are, almost by definition, more likely to be living in poverty.

Perhaps recognizing that some people fall between the cracks of FCRA legislation, many states have created their own statutes that control the commercial mining and use of government's criminal justice data. These various state approaches, ordered by concept, are set forth in the following section of this report.

---

[22] *Criminal Records and Employment in Minnesota, Report and Recommendations of the 2007 Collateral Sanctions Committee*, Minnesota Sentencing Guidelines, 2008

[23] See, *e.g.*, Appendix F, which shows a web site offering "discreet" , "confidential" background checks and a list of sites offering background checks but making no reference to FCRA compliance.

[24] See http://www.criminal-records-search.com/faq.htm, viewed online July 3, 2008.

Overview and Analysis of Identified Approaches

Jurisdictions across the United States have taken different approaches to regulate commercial mining of government's criminal justice data.

Following is a description of those options as reviewed by the Delivery Team. Eight major categories are identified. Each category is briefly described and advantages and disadvantages are listed. If the approach has been implemented in other states, those examples are included.

The Delivery Team working document is found in Appendix E.

I. Limiting information available and removing outdated records

All Minnesota government data about people are considered open to the public unless classified otherwise by law. The Legislature can classify data as *confidential* (accessible only to the keeper of the data, as is the case with active police investigations) or as *private* (accessible both to the keeper and the subject of the data, as are many medical records). These classifications can change over time depending on circumstances or operation of law.

One way to limit the collateral effects of a criminal justice system record is to change its data classification. For example, a public arrest record for a minor matter could, after time, be reclassified as a private record. Timing of this sort of reclassification could be controlled by the Legislature, and could vary by severity level (for example, a minor matter could be reclassified as private sooner than a more serious matter).

Of course, as soon as a government record is reclassified, previously-mined versions of that record are out-of-date or stale. It would do little good to classify a government record as private if its earlier, public version continued to be disseminated by data miners. For this reason, any plan to reclassify criminal justice system records would have to include updating stale, out-of-date data miner records.

1. Analysis

Advantages	Disadvantages
• Provides a more consistent schedule of classification; this could reduce risk and liability resulting from noncompliance. • Reduces the chance that old arrest records will affect employment opportunities for persons never charged or convicted. • Permits an individual who rehabilitates to become a productive member of society. • Respects court decisions so that, for example, when a judge dismisses a case or imposes a minor sanction, the	• Constrains how businesses use public data; this could be considered a violation of the First Amendment guarantee of free speech. • Creates possible confusion for those data miners already regulated by FCRA. • Creates lengthy debate about an acceptable timetable to be used to age-out an old record. • Requires extraordinary amount of cooperation, enforcement, or both to remove outdated records held by thousands of data miners.

individual actually experiences a less harsh outcome over time. • Increases consistency, integrity, and reliability of data if the approach is uniformly implemented across all agencies. • Acknowledges government's responsibility to classify the data it creates. • Addresses the unfairness that results when irrelevant, old data affects an individual's future opportunity. • Reduces the chaos that results when government agencies inconsistently classify the same data. • Permits use of Data Practices Act's already-existing enforcement mechanisms. • Protects presumption of innocence by removing old, unproven allegations.	• Coordinating across various state and local government agencies would be a struggle, since they now operate with inconsistent classification schemes (for example, an arrest record is now public at the local level and private at the state level). • Limits the ability to track behavior important to data customers, such as whether an individual has a history of multiple domestic abuse arrests. • Imposing uniform standards across the branches of government could violate the constitutional separation of powers. • Requires costly data infrastructure changes both by government and data miners. • Limits public's ability to know what government is doing. • The proliferation of sites offering versions of criminal records has made any attempt to regulate or control dissemination impossible. The recent addition of a free (advertising supported) site is an example. Reviewing this site for Minnesota cases shows that some high profile cases are not present, raising questions about why and what this does to the right of the public to information

2. Examples showing how the approach has been implemented

- **California:** consumer reporting agency may not report convictions more than seven years old. It is forbidden to ask job applicants about arrests not leading to conviction, sealed or expunged convictions, or successfully completed pretrial diversions; see Cal. Code of Regulations, Title 2, Div. 4, Ch.2, Subch. 2 §7287.4 (d)(1)(A-C).
- **Montana:** Consumer reporting agency may not report arrests or convictions more than seven years old; see Mont.Code Ann. 31-3-112, "Obsolete information" (2007).
- **Nevada:** Nevada Revised Statutes 598C.150 (2) – Purging of information from files of Reporting agency; disclosure of purged information. "A reporting agency shall periodically purge from its files and after purging shall not disclose: (2) except as otherwise provided by a specific statute, any other civil judgment, a report of criminal proceedings, or other adverse information which precedes the report by more than seven years."

- **Kentucky:** Non-conviction data is only disseminated to criminal justice agencies or for research purposes. 502 KAR 30:060
- **Idaho:** Arrests that have no disposition after 12 months can only be disseminated to criminal justice agencies, the subject of the record, or to someone with a release from the subject of the record. § 67-3008
- **Louisiana:** Strictly limits the dissemination of reports containing non-conviction records. § 548
- **Nebraska:** Except for a few situations, nonconviction data is removed from the public record. § 29-3523
- **Montana:** Mont. Code Ann. 46-18-204 (2007): after dismissal following deferred imposition of sentence, all records and data relating to the charge are confidential and public access may be obtained only by court order. "Public access" likely means access from the court itself, not public access from a data miner.
- **Illinois:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see 775 ILCS 5/2-103.
- **Washington:** Records of arrest, indictments, or conviction of crime older than seven years from the date of disposition, release, or parole date dissemination prohibited. RCW 19.182.040.

II. Regulate data miners

A. "Data refresh" approach

Refreshing data requires data miners at prescribed intervals to obtain and use the most up-to-date government data available. This helps ensure that data miners' records reflect as closely as practical what is on file at the government source.

1. Analysis

Advantages

- Recognizes that criminal justice data are always changing and that any "snapshot" of data soon becomes inaccurate.
- Increases accuracy and integrity of data used to make important decisions, including those that protect public safety.
- Respects the criminal justice system's decision-making process by increasing the likelihood that only the most current records are utilized.
- Allows people who have been cleared (or who end up with only a minor record) the chance to become more fully contributing members of society, rather than forever facing the

Disadvantages

- Creates problems with monitoring compliance and enforcing sanctions because data miners exist in many forms and many jurisdictions.
- Increases costs both for government and for data miners if required to refresh records more frequently.
- Responding to increased demand for refreshed data may not be possible for some government agencies.
- Imposes cumbersome data refresh requirements as inconsistent data about the same event may be held by various agencies due to error or because each agency's business function is different.
- Constrains how businesses use

inferences caused by an accusation.	public data; this could be considered a violation of the First Amendment guarantee of free speech.

2. Examples showing how the approach has been implemented

- **Minnesota:** Chapter 315 from the 2008 legislative session will require business screening services to update their data from the source monthly as of July 1, 2009.
- **Connecticut:** Public Act 07-243 requires background screening services to update their data *at the time* they provide it to the data customer. In 2008, this was amended to require refresh of data *every 30 days*.
- **Alaska:** Nonconviction data is limited in its dissemination. All information disseminated has to be verified as the most updated information, the person who requests the information is kept on file, and it may only be used for the purpose it is requested. Sec. 12.62.160

B. Impose no regulations on data mining entities and allow the market to self-regulate

State government regulation of data mining would come at a cost: expense for taxpayers, extra effort for government agencies, burden on private enterprise, and possible unintended consequences. With these potential outcomes in mind, the delivery team considered the alternative: doing nothing.

If the State of Minnesota were not to regulate data miners, perhaps the market would self-regulate. In cases where it did not, people unfairly disadvantaged might be able to learn how to protect themselves by filing federal lawsuits under the Fair Credit Reporting Act.

1. Analysis

Advantages	Disadvantages
• Imposes no cost on government and no burden on data miners or their customers. • Creates no areas of potential conflict with federal law. • Avoids possibility that state limitations on record availability could create a secondary market for historically accurate records.	• This approach has not resulted in consistently reliable, accurate and complete data. • Data subjects would continue to face unintended consequences from criminal justice system records. • Commercial data miners have no economic incentive to protect the interests of data subjects. • Keeps errors in data from being visible to the data customer and misuse of data from being visible to the data subject; these factors make market self-regulation less likely.

2. Examples showing how the approach has been implemented

Historically, the State of Minnesota has not regulated data miners; this approach is the *status quo.*

C. Certify and train commercial users

Minnesota could create a system to train and certify data miners of the Minnesota criminal justice system data. Failure to either train or receive certification could result in the disqualification of the parties to receive future data. Training would also be provided to the users of the data so they understand the significance of the information they have.

1. Analysis

Advantages	Disadvantages
• This approach would provide standardization of information being presented • This is an opportunity to educate on legal and illegal use of criminal justice records • This approach would provide standardization of information. • Only trained and/or certified parties could receive data. • Better understanding of the criminal justice data by commercial users	• Costs to state to provide training/Certification program. • Additional cost to taxpayers. • Requires constant monitoring of both miners and users. • Difficult to enforce against users of data.

2. Examples showing how the approach has been implemented

- Massachusetts: Executive Order 495 requires Non-Criminal Justice and Private entities accessing data to be certified, and to receive training to maintain certification.[25]

D. Allow criminal justice system records to be disseminated only with the informed consent from data subjects.

To ensure effective management of individual criminal justice record information, there must be a way for individuals to have knowledge when entities attempt to access their criminal justice records and for what purposes it is being accessed. Informed consent would allow the ability to block such access if it is not statutorily authorized and also give the individual opportunity to review and correct incorrect information potentially disseminated.

1. Analysis

Advantages	Disadvantages
• None were proposed.	• Illogical. No person with a criminal record would consent to have their record made public. • Many of these records are public and accessible. • Decreases public safety and detracts

[25] See http://www.mass.gov/Agov3/docs/Executive%20Orders/executive_order_495.pdf, viewed online August 5, 2008.

	from an informed society. • Prohibitively costly to acquire consent in all cases.

2. Examples showing how the approach has been implemented

- **Illinois -** (20 ILCS 2635/7 (A) (1) (2) (from Ch. 38, par. 1607) – Illinois Uniform Conviction Information Act. A requester shall, in the form and manner prescribed by the Department (Illinois Department of State Police), submit a request to the Department, and maintain on file for at least 2 years a release signed by the individual to whom the information request pertains.

III. Apply Fair Information Practice Principles to the Private Sector

The Fair Information Practice Principles (FIPPs) provide a broad set of policies designed to guide use of government-held data about individuals. The FIPPs are reviewed in the earlier section of this report titled *Background.*

It is central to FIPPs that data subjects should receive notice about whether and how data about them are used, and that they be given an opportunity to dispute the accuracy and completeness of records. This principle also forms the foundation of Minnesota's government data policy.[26]

Minneapolis and St Paul ordinances provide examples that demonstrate how such notice provisions are put into practice in the private sector. In those cities, law already requires landlords who accept application fees to give written notice to applicants advising them about the criteria on which their application will be judged. If a tenant is rejected, the landlord must "notify the tenant in writing of the reasons for rejection, including any criteria that the applicant failed to meet, and the name, address, and phone number of any tenant screening agency or other credit reporting agency used in considering the application."[27] If applied to employers, such a notice provision could provide additional protection to employees otherwise dismissed without explanation.

All users of data mined from the criminal justice system could be required to provide data subjects with notice and an opportunity to correct records.

[26] Statutes regulating government-held data provide subjects with the opportunity to be notified about their right to access government data (MS§13.05, Subd. 8), to view such data about them (see MS§13.873 and MS§13.04), and to be able to challenge data that are not accurate or are incomplete (MS§13.04).
[27] St. Paul City Code §54.03; Minneapolis Code of Ordinances §244.1919(16)(c)

A. Analysis

Advantages	Disadvantages
• Embodies well-accepted set of principles designed to guide use of government data. • Imposes no direct cost on government or data miners. • Places obligation on data consumers, who have closest contact with data subjects and are therefore in the best position to provide notice. • Informs people about the source of information affecting them. • Enhances quality of both government and data miner records by allowing data subject to dispute incorrect or incomplete data. • Discourages ineligible people from submitting applications.	• Creates possible confusion for those data miners already regulated by FCRA. • Fails to deter those who willingly break the law. • Creates additional burden to require notice of the criteria on which an application will be judged. • Slows down the application process for landlords and employers and creates greater cost for them. • Causes expense for landlords and employers as they must track addresses of all applicants in order to send notices. • The notice of all disqualifying offenses is onerous. • Removes discretion for employers and landlords to give an offender a break.

B. Examples showing how the approach has been implemented

- **Minnesota:** Applies some FIPPs to the private sector; see, e.g., MS§325E.61 (security breach notification).
- **Minneapolis and St. Paul:** Ordinances already require landlords who take application fees to give lease applicants reasons for rejection, criteria used, and contact information for the data miner utilized, see St. Paul City Code §54.03; Minneapolis Code of Ordinances §244.1919(16)(c).
- **California:** California's "FCRA Plus" statute gives data subjects greater rights to see the results of background checks, increasing the chance that incomplete or inaccurate information can be corrected. California FCRA-Plus gives data subjects rights when affected by data miners not covered by federal FCRA, such as Web sites offering to find "anything out about anybody." See California Civil Code §1786
- **Indiana**: Indiana allows individuals to review their information for mistakes and if a mistake is found, the individual can get a list of all the non-criminal justice agencies that have been given the information. 240 IAC 6-1.1-5.
- **Georgia:** Georgia Crime Information Center Records. In the event that an employment decision is made adverse to a person whose record was obtained pursuant to this code section, the person will be informed by the business or person making the adverse employment decision of all information pertinent to that decision. Failure to provide all such information to the person subject to the adverse decision shall be a misdemeanor. GA Code 35-3-34 (3) (b)
- **Vermont:** Puts strict requirements on the dissemination of records to employers including requiring that the person must be given a conditional offer before a background check can be run. Additionally, there are a series of releases required to

be signed by the subject of the search. Administrative code also puts restrictions on the dissemination of nonconviction records. § 2056c and 28.050.001.

IV. Improve Accuracy of Records

Uniform data entry standards and definitions for government criminal justice records could increase quality of source data and reduce negative effects on individuals once those data are mined.

A. Analysis

Advantages	Disadvantages
• Improves quality of data, thereby resulting in better decisions. • Reduce discrepancy of information between government sources. • Increases accuracy and reliability of records.	• Increases cost to government by changing its data infrastructure. • Creates possible violation of the constitutional separation of powers by imposing uniform standards across the branches of government. • Requires significant training for data entry personnel.

B. Examples showing how the approach has been implemented

- **Minnesota**: The court system has built a single statewide information system over the past several years, called the Minnesota Court Information System (MNCIS). MNCIS provides a level of standardization not possible in the courts' previous county-based system. This standardization effort is limited to the Judicial Branch.
- **Minnesota:** The court system has built a single statewide information system over the past several years, called the Minnesota Court Information System (MNCIS). MNCIS provides a level of standardization not possible in the courts' previous county-based system. This standardization effort is limited to the judicial branch.
- Department of Justice Regulations establishes minimum criteria for disposition reporting. To be "complete," an arrest record must contain disposition information within 90 days of dispositions. 28 C.F.R. 20.21(a)(1)
- **Colorado:** A privacy-friendly law requiring the credit bureaus themselves to provide annual notices to any consumers who have had negative information added to their reports. 12-14.3-104. Disclosures to consumers.
- **Connecticut:** Connecticut, State Substitute Senate Bill No. 1089 Public Act No. 07-243 Effective January 1, 2008. Amended by Public Act No. 08-53. All Consumer Reporting Agencies (Background Screeners) must confirm criminal records found on those in the state of Connecticut (on a site provided by the state) and maintain procedures designed to ensure that any criminal matter of public record reported is complete and up-to-date as of the date the consumer report is issued,. The CRA must also notify the subject of the report about the presence of the records being reported. http://www.cga.ct.gov/2008/ACT/Pa/pdf/2008PA-00053-R00SB-00704-PA.pdf
- **Maine**: MRS Title 10 Part 3 chapter 210 §1321 2. Prohibited information, accuracy of information in reports. Accuracy. Whenever a consumer reporting agency prepares a consumer report, it shall follow reasonable procedures to assure maximum possible

accuracy of the information concerning the individual about whom the report relates and refrain from reporting inaccurate information and information which cannot be verified, unless efforts to verify the information are also contained in the report.

- **Montana:** 44-5-213. A criminal justice agency shall query the state repository prior to dissemination of any criminal history record information to ensure the timeliness of the information. When no final disposition is shown by the state repository records, the state repository shall query the source of the document or other appropriate source for current status.

V. Limit Uses of Data, Provide Remedies

Consequences of a criminal record can sometimes be unjustly severe on the data subject and costly for society. Methods are detailed below which could be used to lessen the severity of these outcomes.

A. The CORA approach

Minnesota's Criminal Offender Rehabilitation Act (CORA)[28] currently mitigates employment consequences by limiting government employers' ability to use criminal justice system records to affect the hiring process. CORA's limitations do not apply in circumstances where statutes mandate a pre-employment background check.

Similar legislation could impose CORA-like limits upon private employers and/or landlords. The Minnesota Legislature in 2008 considered language that would have extended CORA to private employers, but the bill did not become law.

1. Analysis

Advantages	Disadvantages
• Creates consistent rules that apply to both private and public sector employers. • Provides protection for people who otherwise would be unemployed due to arrest or conviction unrelated to their ability to do the job in question. • Maintains the full public record; that is, this approach limits the *use* of criminal justice system records, not their *availability*. • Helps block any occurrence of racial discrimination in the justice system from being replicated in the hiring process.[29]	• Constrains how businesses use public data; this could be considered a violation of the First Amendment guarantee of free speech. • Lowers the bar for entry into the workforce, thereby increasing the possibility that a dangerous person could get into a job where they could hurt someone. • Affects employers only, a narrow segment of the population of data consumers. • Increased risk to the public by dangerous people getting jobs and housing that puts others at great risk.

[28] M.S.§346.01 *et seq.*

[29] Minnesota's Legislature has found that "the reality or public perception of racial profiling alienates people from police, hinders community policing efforts, and causes law enforcement to lose credibility and trust among the people law

- Employers will be less likely to hire African American workers, especially men.[30]

2. Examples showing how the approach has been implemented

- **Arizona:** Civil rights law limits an employer's inquiry of an applicant regarding prior convictions. The employer must include a statement that a conviction will not be an absolute bar to employment. See http://www.azag.gov/civil_rights/PreEmploymentInquiriesGuide.pdf.
- **California:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Cal. Civ Code 1786.18(a)(7).
- **Colorado**: Civil rights law allows employers to question about convictions only if all applicants are questioned in this manner; employers may only make hiring or retention decisions based on actual convictions are substantially related to applicant's ability to perform a specific job. http://www.dora.state.co.us/civil-rights/Publications/JobDiscrim2001.pdf
- **Hawaii**: Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; further, employers can consider only rationally related convictions occurring in the past 10 years, and then only after conditional offer of employment. Haw. Rev. Stat 378-2.5.
- **Kentucky**: No consumer reporting agency shall maintain any information in its files relating to any charge in any Kentucky criminal case unless the charge has resulted in a conviction. See KRS Chapter 367.00 §310.
- **Rhode Island**: Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Rhode Island Gen. Laws. 28-5-7(7).
- **Wisconsin**: Fair employment law prohibits firing or disqualification from employment because of arrest or conviction unless the arrest or conviction is substantially related to the employment. See Wisconsin Statutes. 111.31-111.395 or, for more specific information, http://dwd.wisconsin.gov/er/discrimination_civil_rights/fair_employment_law.htm

B. Restrict dissemination of nonconviction records

Since many users of criminal justice data do not understand the difference between an arrest record and a conviction, people who are arrested, but never convicted (and in many

---

enforcement is sworn to protect and serve." M.S.§626.8471. When the private sector hiring process relies unquestioningly on law enforcement records, it is subject to the same unfairness or perception of unfairness.

[30] This result could occur if a CORA-like restriction on the *use* of conviction data was ever expanded by the Legislature to restrict *access* to conviction data. Research suggests that, if employers have no access *to* criminal background checks, they tend to assume the worst about African-American job applicants. See http://www.jjay.cuny.edu/centersinstitutes/pri/pdfs/HolzerStollRaphaelBackgroundChecks2006.pdf, viewed online August 5, 2008. Strahilevitz, Lior, *Privacy versus Antidiscrimination*. University of Chicago Law Review, Vol. 75, 2007 Available at SSRN: http://ssrn.com/abstract=1003001

cases, never even charged) may find that the arrest alone is used to disqualify them from either housing or a job. One solution would be to make the name and other identifying information private until charges are filed or a conviction is obtained.

1. Analysis

Advantages	Disadvantages
• Presumed innocence until proven guilty. • Non-conviction records are not proof of guilt. • May reduce potential for discrimination. • Individuals would not be denied opportunities (e.g. housing, employment, based on arrest not resulting in a conviction).	• Increased risk to the public by limiting information which is relevant in assessing risk. • Limits access to records of defendants charged with the most serious offenses because serious cases routinely take over a year to reach a disposition. • Applicants may be tempted to lie on applications when asked if they have ever been charged. This falsehood could eliminate them from consideration when the fact they were charged would not have eliminated them. Lying on certain documents and in certain circumstances is a crime. • Removes government accountability by removing record of government activity. • First Amendment Freedom of the press issue. • Freedom of Information Concern. • Repeat arrests would be completely hidden. Rental housing providers can lose their license based on the conduct of residents and their guests. • Difficult to implement. An arrest many be public for a specified length of time unless it resulted in a conviction. Law enforcement agencies do not necessarily track an arrest through disposition, so determining the classification would be cumbersome.

2. Examples showing how the approach has been implemented

- **California, New Mexico and New York** preclude the reporting of arrests that do

not result in convictions: California - Cal. Civ. Code § 1786.18(a)(7); New Mexico - N.M. Stat Ann. § 56-3-6(a)(5); and New York – N.Y. Bus. Law § 380-j(a)(1).

- **Colorado**: CRS 12-14-.3-105.3 (1)(e) – Reporting of information prohibited: No consumer reporting agency shall make any consumer report containing any of the following: Records of arrest, indictment or conviction of a crime that, from the date of disposition, release, or parole, predate the report by more than seven years.
- **Connecticut:** GSC Title 54 Chapter 961a Sec. 54-142n and Sec. 54-142o Criminal Records. *Sec. 54-142n*. Nonconviction information other than erased information may be disclosed only to criminal justice agencies, the federal government court order or by statutory authority. *Sec. 54-142o.* Nonconviction information disseminated to noncriminal justice agencies shall be used by such agencies only for the purpose for which it was given and shall not be redisseminated. No agency or individual shall confirm the existence or nonexistence of nonconviction information unless authorized.
- **Kansas:** KS Chapter 50 Article 7 – Fair Credit Reporting – 50-704 No consumer reporting agency may make any consumer report containing any of the following items of information: records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years. There is a employment salary exception.
- **Kentucky**: KRS Chapter 367.310 – Consumer reporting agency records restriction. No consumer reporting agency shall maintain any information in its files relating to any charge in a criminal case unless the charge has resulted in a conviction.
- **Maryland:** Code of Maryland §14-1203 (a) (5) - Reporting of obsolete information prohibited Except as authorized no consumer reporting agency may make any consumer report containing any of the following items of information: Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years. There is an employment salary exception.
- **Michigan**: Michigan Compiled Laws Act 453 of 1976 §37.2205 a §205a (1) An employer, employment agency, or labor organization, other than a law enforcement agency of this state or a political subdivision of this state, shall not make or maintain a record of information regarding a misdemeanor arrest, detention, or disposition where a conviction did not result. A person is not guilty of perjury or otherwise for giving a false statement by failing to recite or acknowledge information the person has a civil right to withhold by this section. This section does not apply to information relative to a felony charge before conviction or dismissal.

C. Authorize state attorney general to enforce law affecting data mining process

The attorney general could be authorized to bring suit against either data miners or their customers or violations of any laws affecting the data mining process. The action could

be for either injunctive relief or damages. Federal law (15 U.S.C.A. s [c]) already allows the attorney general to bring actions either in law or equity for violations of FCRA.

1. Analysis

Advantages	Disadvantages
• Provides a central authority with resources available to take action. • Provides legal assistance to those who cannot afford an attorney. • Allows expertise to be developed in one location in state. • People know where they can receive legal assistance. • Would vest a considerable amount of enforcement power in the hands of the AG's Office which is already granted powers under FCRA.	• There will be costs for implementation, and implications for the number of needed Attorney General staff. • Duplication of the law since federal law already gives authority to enforce FCRA. • To avoid preemption would need to work in conjunction with FCRA. Right already granted under FCRA.

2. Examples showing how the approach has been implemented

- Examples include State Security Breach legislation and State Credit Reporting Requirements that are not part of FCRA

D. Give data subjects the ability to sue data miners.

The subject of the data could be granted a cause of action to recover damages for either negligence or intentional dissemination of false information. This might allow for the recovery of attorney's fees if the action is brought to a successful conclusion.

1. Analysis

Advantages	Disadvantages
• Allows for enforcement of statutes without cost to the taxpayers. • Additional means for individual to obtain retribution if they are harmed. • Deterrent to not complying with statute	• Costs of litigation will be passed on to customers. • Costly to taxpayers if false information traced back to a governmental entity. • Difficult to prove. • Potential for abuse and frivolous lawsuits. • Significant enforcement authority already exists under FCRA for the FTC and AG's Office.

2. Examples showing how the approach has been implemented

- None Found

VI. Education

Generally, there is a lack of understanding about laws affecting data mining. Data subjects, lawyers, and the public in general have limited awareness about the rights and obligations of the data miner, data consumer, and data subject under federal and state law.

A. Create a state agency

Minnesota's Legislature could create and fund a state agency with the duty to educate about state and federal law. The agency could be funded by registration fees on data miners registering to do business in Minnesota. An alternative method of funding could be to create a single state source for criminal justice system records, and charge a fee to anyone collecting the records.

1. Analysis

Advantages	Disadvantages
• Reduces confusion about the law. • Creates the ability to enforce enacted laws. • Provides authority to interpret data and maintain a glossary of definitions to help consumers understand mined data. • Certifies users prior to allowing access to data and requires additional training to maintain certification. • Provides information about available remedies for violations. • Monitors and enforces compliance of state regulations by data miners. • Ensures that expunged/sealed records are not available through data miners. • Trains and certifies data miners. • Allows for a better understanding of the criminal justice data by commercial users. • Provides enforcement authority.	• Increases the costs to government and taxpayers. • Creates possible jurisdictional challenges by attempting to regulate data miners in other states and countries. • Creates a partial solution as data miners would still gather information from other states about Minnesotans. • Increases the costs to data consumers and subjects for screening reports. • Creates possible duplication of Federal Trade Commission's efforts to educate people about FCRA.

2. Examples showing how the approach has been implemented

- **California:** Created an Office of Information Security and Privacy Protection (OISPP) in 2000 whose mission is to identify consumer problems in the privacy area and encourage the development of fair information practices. See http://www.oispp.ca.gov. California is the first state to have an agency dedicated to promoting and protecting the privacy rights of consumers. Its mission is to identify consumer problems in the privacy area and encourage the development of fair information practices. The OISPP recommends policies and practices that protect individual privacy rights.
- **Virginia:** On January 7, 2007, Governor Kaine launched an initiative to work with

business and consumer advocates to protect consumer data. http://www.governor.virginia.gov/MediaRelations/NewsReleases/viewRelease.cfm?id=323

- **Ohio:** The State of Ohio Privacy & Security Information Center acts as a privacy and security knowledge center for the citizens, businesses, and employees of the State of Ohio. http://www.privacy.ohio.gov
- **Arizona**: The Statewide Information Security and Privacy Office (SISPO) has, as part of its charge, (under its enabling statute 41-3507) to "[c]oordinate statewide information security and privacy protection awareness and training programs." http://www.azgita.gov/sispo
- **Wisconsin:** Part of the mission of Wisconsin's Office of Privacy Protection is to protect the privacy of individuals' personal information by identifying consumer problems and facilitating the development of fair information practices; to educate the public on potential options for protecting the privacy of, and avoiding the misuse of, personal information; to provide information and assistance, where appropriate, to consumers in reclaiming their identity and clearing their name in the event of identity theft or identity fraud; and others. The office was created by Wisconsin's governor in 2006. See http://privacy.wi.gov; http://privacy.wi.gov/mission/pdf/FactsheetMissionStatement.pdf

B. Survey data subjects

It is quite difficult to count or to survey people who are negatively affected by data mining. Some people disadvantaged by the background check process are simply escorted out the door with no substantive explanation for the termination. They likely have no idea if a data miner was used in the process or not. Others may remain unaware of a background check simply because they do not receive a return call from a potential landlord or employer. There is, however, a segment of this population more likely to be aware of data mining and its effects: that is, people who contact the Minnesota Bureau of Criminal Apprehension (BCA) with requests to correct or complete a criminal history record.

Hundreds of such people contact the BCA every week; of these numbers, about 10 per week are successful in their effort to get their record corrected or made complete. These people could be surveyed to obtain insights about where problems exist in the government process of creating and maintaining records, or where there is a breakdown caused by the data mining process.

During the survey process, the BCA could also provide literature explaining rights under FCRA and state law. People could receive referrals to volunteer organizations to assist in disputing and correcting criminal records. The survey process could then follow up to determine the results of any disputes filed with consumer reporting agencies; document the results and report the results to the Task Force, Policy Group, and Legislature.

1. Analysis

Advantages	Disadvantages

• Provides immediate direct assistance to subjects of data to clean up inaccurate records. • Determines if people are negatively affected by inaccurate records and/or data miners. • Determines where records are inaccurate, source of record or data miner. • Determines if remedies already available under the Fair Credit Reporting Act (FCRA) are effective.	• Increases costs to taxpayers for the study. • Requires additional time needed to complete the study, thereby delaying action to resolve the issue. • Provides limited options for successful follow-up study, given options for contact with people who do not have permanent homes. • Limits conclusions possible due to the availability of a narrow population that could be studied.

2. Examples showing how the approach has been implemented

No examples found.

C. Give data subjects the right to access data miner records

Data accuracy would be improved if data subjects were provided access to their records held by data miners. State law could give data subjects the right to see who has received information about them. This could help data subjects make sure that changes in the record are received by all users.

1. Analysis

Advantages	Disadvantages
• Provides knowledge to the data subjects as to information contained in their record. • Creates transparency of records. • Provides opportunity to contact and correct entities using data.	• Requires data subject action to change records at numerous locations. • Requires data miners to seek out subject to provide copy of record.

2. Examples showing how the approach has been implemented

No examples found.

VII. Sealing and Expunging Records

Data subject rights and data quality would be improved if the state were to implement the Criminal and Juvenile Justice Information Policy Group's recommendations contained in the 2008 Background Check and Expungement Report. By allowing the court to seal executive branch records, these recommendations would reduce the data available to data miners by allowing the court to seal records. Exceptions could be created for domestic assault charges, or when the defendant has, within one year, been convicted of a serious offense (this could be defined as a felony, gross misdemeanor, or targeted misdemeanor).

A. Analysis

Advantages	Disadvantages
• Allows judge who imposes sentence to have more control over actual sanctions. • Allows for the trial court to assist in concept of rehabilitation. • Requires the subject to take some action in case with conviction. • Requires automatic expungement without need for action by subject when case does not result in conviction. • Allows subject to move court in cases where there is disagreement over whether expungement should happen. • Facilitates resolution of cases in the court room. • Gives court authority over Executive Branch records.	• Closes some records that are not relevant for some purposes, but are relevant for other purposes such as day care licensing. • Creates concerns about public safety by allowing potentially relevant records to be expunged. • Eliminates government accountability by hiding arrest records with no conviction. • Reduces value of sealing / expunging of any criminal record because of internet and availability. • Reduces value of sealing / expunging of acquittal because of lack of court and Executive Branch records enabling subject to prove acquittal.
• Creates consistency in expungement policies of Judicial and Executive branches. • Reduces consequences of stale and irrelevant records by making them unavailable. • Removes the burden on data subjects to move the court for an order in some instances. • Requires government entities to cooperate. • Makes exceptions for those with a high need for the data. • Creates an appeals process.	• Creates a false sense of security on the part of the data subject that no record exists. • Creates false belief by data subject and others that expungement is the same as a pardon. • Creates issues of the separation of powers between Judicial and Executive branches, as well as issues with implementation between branches. • Violates the standard of openness of the judicial system. • Requires a definition of the order of transmission, integration across all systems (government and data miners). • Fails to apply sealing to more than just data miners. • Lacks standards to determine what data is relevant. • Attempts to deal with collateral consequences by pretending event didn't happen, instead of addressing collateral consequences directly. • Loses relevance of the behavior of the data subject. • Hampers efforts that utilize valuable

	information from examination of arrest information meaningfully and thoroughly (on the part of some entities) • Creates a private set of records for media and data harvesters unless statute requires its removal. • Creates a fiscal impact for the Judicial and Executive branches by requiring learning standards, making discretionary decisions, and constant review of the tail of downstream dissemination. • Establishes an unfunded mandate for county and city government. • Fails to extend to all public and private repositories. • Requires state to be able to transmit revised data to all public and private entities that previously received the data.

C. Examples showing how the approach has been implemented

- **Texas** - Sec. 411.0851. There is a duty for a private entity to update criminal history information. Civil action may result for failure to do so.
- **Colorado** - CRS 24-72-308. Employers are prohibited from requiring an applicant to disclose any information contained in sealed records. An applicant need not answer any question concerning arrest or criminal records that have been sealed and may state that no such action has ever occurred. An application may not be denied solely because of the applicant's refusal to disclose arrest and criminal records information that has been sealed.
- **Arizona**: 13-4051. Entry on records; stipulation; court order. Any person wrongfully arrested, indicted or otherwise charged for any crime may petition the superior court for entry upon all records that they have been cleared and prohibit dissemination of record. Any person who has notice of such order and fails to comply with the court order issued pursuant to this section shall be liable to the person for damages from such failure.
- **Nevada**: NRS 179.255;245;259;285 Effect - deemed never to have occurred and restores civil rights. May properly answer accordingly to any inquiry, including, an application for employment, concerning the arrest, conviction, dismissal or acquittal and the events and proceedings relating to the arrest, conviction, dismissal or acquittal.

VIII. Charge Fees for Each Record

Government could finance regulation of the data mining industry by charging per-record fees and not providing a bulk discount. Some state agencies currently provide entire databases to data miners with no fee.

1. Analysis

Advantages	Disadvantages
• Provides government with funding based on the commercial value of the data. • Allows regulation of data miners without cost to taxpayers. • Limits collection of data to those with need. • Increases revenue for government.	• Creates an adverse impact on non-FCRA uses of the data (e.g. skip-tracing, law enforcement uses). • Places a financial burden on those who seek public information. • Creates economic disparity allowing people with the means to get public information that other people cannot afford. • Discourages "repositories" or data mining/aggregation. • Constrains how businesses use public data; this could be considered a violation of the First Amendment guarantee of free speech. • Creates conflict with philosophy of freedom of information and the Minnesota Data Practices Act. • Impedes efforts to aggregate data for non-FCRA purposes including law enforcement and academics. • Multiplies the number of system and staff requirements to process record requests and extract single records. • Requires data subjects to pay more for screening due to the increase in costs. • Reduces the number of employers and landlords who screen applicants thereby creating public safety problems.

2. Examples showing how the approach has been implemented

- **Florida**: Each search of criminal justice system records costs $23 and there is no discount for bulk purchase. See http://www.fdle.state.fl.us/CriminalHistory
- **North Carolina**: Criminal histories are available for $14 per record to non-criminal justice requestors.
- **Pennsylvania**: Only if an arrest is less than three years old, no conviction has occurred and no proceedings are pending can it be disseminated to non-criminal justice agencies, and a fee may be charged for each request.

Conclusion

The commercial use of government information by data miners provides a clear set of advantages and conveniences. At its best, data mining makes society a safer place. Yet the inadvertent effects of data mining might be to exaggerate the seriousness of any involvement with the criminal justice system, making good people unable to become fully contributing members of society. Such marginalized people may, ironically, be more likely to become involved in the criminal justice system. At its worst, then, data mining may make society a less safe place to live. Policy makers are asked to balance the benefits and the disadvantages of data mining to craft a set of rules that protect the subjects and the consumers of data.

Minority Report

I disagree with the overarching premise of the report as characterized in the Overview:

> "..Once information is given out and no longer in government's control, however, mined records often are practically irretrievable and uncorrectable either by government or by the data subject.[31] Many records, designed for use by police and courts and probation officers in the context of a criminal investigation or court case, now are broadly available for use out-of-context by people unfamiliar with the criminal justice system. What is understood as a minor matter by those within the criminal justice system may be perceived as deeply significant by those with little exposure to criminal justice records. Further, once controlled by private and commercial interests, the records can take on a quality of permanence never intended by the criminal justice system, possibly resulting in consequences upon the data subject that are out of proportion with the seriousness of the recorded event…"

The first sentence is factually incorrect. Under the Fair Credit Reporting Act (FCRA) citizens have the right to dispute inaccurate records and companies have the obligation to promptly correct them. The assertion throughout the report that one must hire a lawyer and sue in order to correct inaccuracies is inaccurate. One must simply notify the company of the inaccuracy.

Public records are not created solely for criminal justice agencies to process criminal cases. They document the activities of the government. They provide transparency and accountability. They provide the public with information that they have the right to know. An employer's decision to not hire a criminal is not out-of-context to the safe operation of their business. What a seasoned peace officer considers a minor matter based on their experiences may indeed be deeply significant to an employer or landlord in protecting their business or tenants.

The report implies that when members of the public have access to public information, they make the wrong decisions.

Over my career I have seen a tremendous increase in the information available to criminal justice professionals. Police, prosecutors, defense attorneys, judges and corrections officials are all making better decisions because they are better informed. As a result the public is safer and the administration of justice is fairer. It is logical to assume that the better information the private sector has, the better their decisions also will be.

I believe we need far more information before concluding that there is a problem with data miners. At our first meeting I asked a question I thought should be answered in our work: "Has Data Mining had an adverse affect?"

Our work is done and I do not know the answer. I've spent a considerable amount of time digging into the research and found very little factual information regarding data mining of criminal justice records and its impact on Minnesotans.

[31] The *data subject* is the person about whom information is sought; for example, a job applicant whose background is checked as part of the application process.

No research addressed improved public safety gained by employers and landlords using public information to screen perspective employees and tenants.

Various studies attempt to quantify difficulties that criminals may have finding jobs and housing. Many of the studies reported opinions, not facts. They did not involve data provided by data miners, but rather from government sources. They did not address the other side of the coin; increased risk to the public if certain criminals have certain jobs or live in certain housing situations.

The staff did an excellent job of gathering available research regarding the broad subject of the relationship between criminal activity and employment and housing opportunities. Perhaps the reason we don't have more research regarding data mining is because little exists. The best Minnesota information we have is a BCA estimate that they hear from 1 or 2 citizens a week who are inquiring about issues related to data mining.

I believe any problems should be articulated, quantified and the consequences of any proposed legislation be fully explored before any laws are changed.

The team did hear a very informative presentation regarding the Fair Credit Reporting Act. I discovered that I was largely unaware of the rights of consumers under the act as well as the obligations of reporting agencies, employers and landlords. I believe we should have a solid understanding of existing federal law before passing new state laws that may complicate matters.

We should pinpoint any existing problems and explore all potential solutions before passing any new legislation. Companies who violate an existing federal law would probably violate a new state law. People unaware of their rights under an existing federal law would probably be unaware of their rights under a new state law. Enforcement and education may be more effective then legislation.

We should focus on identifying where legislation truly may be needed. For example, web sites that offer free searches may not be covered under FCRA and perhaps focused state legislation could offer citizens "FCRA-like" protections. Legislation narrowly focused to address specific problems is less likely to result in negative unintended consequences then broad sweeping changes.
The Data Mining Delivery Team was convened to study data mining. Nine 3-hour meetings were planned to complete the work. The scope of the team's discussions expanded far beyond data mining.

The report contains approaches that are unrelated or only tangentially related to data mining. For example, Approach III, Apply Fair Information Practice Principles to the Private Sector, involves regulating landlords, not data miners. Approach V, Limit Uses of Data, Provide Remedies, is largely unrelated to data mining. It discusses expanding Minnesota's Criminal Offender Rehabilitation Act to regulate all employers and landlords in Minnesota. It also discusses restricting government's dissemination of what have been public records since this country was founded. We should have very compelling reasons before restricting the free flow of what is currently public information. In my opinion no compelling reasons for new restrictions were presented to the team.

The report fluctuates between correcting inaccurate records and restricting the dissemination and use of accurate records. There is no disagreement that public records should be accurate. My experience is that they are extremely accurate.

However, restricting dissemination and use of public records are major policy decisions requiring intensive study and thoughtful deliberation. These issues deserve far more consideration and discussion then the 27 hours the team met to discuss them.

Hopefully the advantages and disadvantages listed in the report help provide a starting point for serious, in-depth, inclusive discussion of these issues before any legislation is considered.

I thank the Delivery Team members for our friendly, respectful discussions regarding serious and controversial issues. Also thanks to David Anderson and Tracy Fischer for their professional staff work.

Sincerely,
Dave Fenner
Commander, Ramsey County Sheriff's Office

Appendix A

Fair Information Practice Principles and the Private Sector
Data Mining Delivery Team
April 30, 2008

General background information

The Fair Information Practice Principles (FIPPs) were first published in *Records, Computers and the Rights of Citizens: A Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973, U.S. Department of Health, Education and Welfare).

The principles are:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for individuals to find out what information about them is in a record and how it is used.

3. There must be a way for individuals to prevent information about them that was obtained for one purpose from being used or made available for other purposes without their consent.

4. There must be a way for individuals to correct or amend a record of identifiable information about them.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Similar principles were published in Great Britain in 1972.

Beginning in 1973, European countries began enacting privacy laws using the FIPPs that are applicable in both the public and private sectors. In 1980, a convention of the Council of Europe adopted privacy protections using the FIPPs as did the Organization for Economic Cooperation and Development (www.oecd.org).

In 1995, the European Union issued a directive on personal data that required both public and private sector recipients of data about Europeans to provide the same privacy protections as required by European law (http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm). As a result, a "safe harbor" agreement was reached between the EU and the USA to allow the cross-Atlantic transfer of personal data (http://www.export.gov/safeharbor/sh_overview.html).

Most recently, Canada adopted a private sector privacy law in 2000 that incorporates the FIPPs (the Personal Information Protection and Electronic Documents Act or PIPEDA;

http://www.privcom.gc.ca/legislation/02_06_01_e.asp). This law covers any private sector commercial activity and health information. Journalism is explicitly exempted.

The FIPPs continue to be a foundational element when consumer privacy is considered. In a report to Congress in 2000 about privacy in the electronic marketplace, then Federal Trade Commission Chairman Robert Pitofsky said: "There is now wide agreement on the required elements of privacy protection, referred to as the Fair Information Practice Principles." Chair Pitofsky went on to list the principles as: notice, choice, reasonable access and adequate security. (See http://www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.shtm)

The Data Mining Delivery Team has identified two problem areas that coincide with the FIPPs. Each is presented below, along with examples of United States laws that use the stated FIPP.

Access problem

> FIPP 2. There must be a way for individuals to find out what information about them is in a record and how it is used.

Examples of FIPP 2 application in the private sector:

Health Insurance Portability and Accountability Act (HIPAA) – 45 CFR section 164.524 (individual access to personal health information)

Fair Credit Reporting Act (FCRA) – 15 USC section 1681g (requires file disclosure to individual)

Fair and Accurate Credit Transactions Act (FACTA) – one free credit report every 12 months from Experian, TransUnion and Equifax.

Integrity problem

> FIPP 4. There must be a way for individuals to correct or amend a record of identifiable information about them.
>
> FIPP 5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Examples of FIPP 4 and FIPP 5 application in the private sector:

Health Insurance Portability and Accountability Act (HIPAA) – 45 CFR section 164.526 (amendment)

Health Insurance Portability and Accountability Act (HIPAA) – 45 CFR section 164.302- .318 (security standards)

Financial Modernization Act of 1999 (Gramm-Leach Bliley or GLB) – 15 USC sections 6801-6809 and 16 CFR Part 314 (safeguards for information)

Fair Credit Reporting Act (FCRA) – 15 USC section 1681i (procedure when accuracy disputed)

Fair Credit Reporting Act (FCRA) – 15 USC section 1681c (limits amount of time negative and bankruptcy information can be reported)

Business sectors covered by the various U.S. laws

HIPAA: health insurance companies, health care providers who do electronic transactions and health care clearinghouses

GLB: all financial institutions including banks, non-federally insured credit unions, insurance companies, brokerage firms, mortgage lenders, "pay day" lenders, mortgage brokers, finance companies, non-bank lenders, check cashing services, collection agencies, and tax preparation services

FCRA and FACTA: "consumer reporting agencies" a/k/a credit bureaus, tenant or employment screening services, agencies with check writing history, agencies that compile medical history, homeowner and auto insurance claims history.

Prepared by:
Katie Engler
Information Policy Analysis Division
MN Dept. of Administration

Appendix B

Further study of federal preemption issue

Using Minnesota Senate counsel's legal research about FCRA as a starting point, the delivery team examined whether FCRA might have the effect, through operation of the federal preemption doctrine, of invalidating state regulation of data mining.

To learn more about FCRA, the Delivery Team accepted an offer from the Consumer Data Industry Association (CDIA) to provide an educational seminar. The CDIA is an organization that represents data miners in Congress and before state legislatures. Stuart K. Pratt, CDIA President, provided a three-hour session for delivery team members and interested parties. We learned that state action is preempted when *adverse action* is taken based on a *consumer report* created by a *consumer reporting agency*.[32] However, outside these defined circumstances, state regulation is possible.

Mr. Pratt acknowledged that, in addition to the population of consumer reporting agencies that consider themselves regulated by FCRA, there is a segment of the industry that operates outside FCRA (though, Mr. Pratt clarified, "that is a business model we do not represent"). Such non-FCRA-regulated data mining is a proper object of state regulation.

That a motivated group of subject matter experts should need to spend many hours debating the nuances of federal law and its relationship to the states should illustrate to the reader why this is a problematic area of public policy. "If a roomful of lawyers has to work this hard to understand FCRA, how can we expect small employers to know what is the right thing to do?" asked Doug Johnson, the delivery team chair and Washington County Attorney.

To get an idea of the sorts of protections Minnesota law might provide in circumstances not covered by FCRA, the delivery team needed first to understand what protections FCRA provides when it does apply. When FCRA applies, consumers have a right to the following:

- Accurate information. A consumer reporting agency must have reasonable procedures to be certain that as much of their data as possible is accurate. 15 U.S.C. section 1681e(b).
- Access to the information. A consumer can see all the data about them at the consumer reporting agency at the time they ask. 15 U.S.C. section 1681g(a).
- The right to challenge the accuracy or completeness of data and to make the challenge without a fee. If a challenge is made, the consumer has the right to see the results of the investigation by the consumer reporting agency and to submit a 100-word statement if they are not satisfied with the result. 15 U.S.C. section 1681i.
- The right to expect that the information about them will only be used for the purposes permitted by FCRA. Examples of permitted purposes include employment, housing, credit, child support enforcement, receipt of a government benefit or any other use requested by the consumer in writing. 15 U.S.C. section 1681b.

[32] Italicized words are highly-specific FCRA terms that are discussed in depth later in this section.

- If the use is for employment, the consumer must be told before the employer asks for the consumer report and the consumer must give permission. 15 U.S.C. section 1681b(b).
- The right to have obsolete negative information removed. Negative information that has a date more than seven (7) years before the date of the consumer cannot be included. (15 U.S.C. section 1681c(a)(5)). The exceptions to this general rule are that bankruptcy information can be included for ten (10) years (15 U.S.C. section 1681c(a)(1)) and convictions are never excluded. (15 U.S.C. section 1681c(a)(5)).
- The right to be notified if a negative action is taken (15 U.S.C. section 1681m).

If an adverse action is taken against a consumer, the consumer has the following additional rights[33] found in 15 U.S.C. section 1681g:

- A right to request free file disclosure.
- A right to be notified that a consumer report has been used as the basis for the adverse action.
- A right to be told which consumer reporting agency provided the consumer report and how to contact it.
- A right to dispute the accuracy and completeness of the data. There is no limit on the number of disputes that can be made by the consumer.
- A right to place a 100-word statement in their file if they disagree with the outcome of their dispute.

If they are not afforded these protections, data subjects *who are aware that they have been aggrieved* by a FCRA-regulated report can retain a lawyer to file a federal lawsuit. However, because the data subject may have no way of knowing that an opportunity was denied and would have limited opportunity to prove what did and did not occur during the decision-maker's evaluative process, the remedies provided by FCRA may not be particularly helpful to the data subject.

None of the criminal justice system subject matter experts participating in the delivery team was familiar with a circumstance in their work where a data subject pursued rights and remedies under FCRA. The CDIA was asked about the incidence of such lawsuits, but that organization has not tracked those data.[34]

The following section of the report identifies what FCRA does and does not control, and further identifies circumstances where the Minnesota Legislature could set different or additional rules.

When state regulation does not conflict with FCRA

Even though FCRA exists, it is possible to create state regulation which addresses data mining-related activity where either (1) no *consumer reporting agency* is involved; (2) *no consumer report* is created; and/or (3) no *adverse action* is taken. Federal definitions of these terms are somewhat circular and cross-dependent. These definitions are examined in detail below.

1. **When no consumer reporting agency is involved.** The FCRA definition of "a consumer reporting agency" is anyone that collects or evaluates consumer information to be able to provide consumer reports to a third party for some kind of compensation and provides the services across

[33] There are additional consumer rights that do not fit the scope of the delivery team's work.
[34] The CDIA does not track filing or settlement of FCRA lawsuits. Email from Jennifer Flynn, CDIA Director of Government Affairs, 7/1/2008.

state lines (15 U.S.C. section 1681a (f)) This definition does not provide a stand-alone answer; rather, it is dependent upon resolution of the question whether a consumer report is created. State regulation is possible in circumstances where, for example:

- Free background checks are provided;
- Where no consumer report is created;
- Where a landlord or employer performs her own investigation; or
- Where the service is offered only to third parties located within the same state as the data miner.

2. **When no consumer report is created.** The FCRA definition of "a consumer report" is a written or oral communication by a "consumer reporting agency" (see immediately above) that is about a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living that is or will be used to make a decision about the consumer's:
    - Ability to get credit or insurance that will be used for themselves or their family,
    - Employment (hiring, promotion or firing); or
    - Other purposes authorized by FCRA. (15 U.S.C. section 1681a(d))

There are some exceptions to the general rule. Examples of FCRA-regulated uses include: credit transactions; for employment decisions; to underwrite insurance policies; to enforce child support obligations or to follow the written directions of the consumer. Examples of other purposes are found in 15 U.S.C. section 1681b. How the data provided by the data miner are *used* determines whether FCRA applies. If a background check report is not used for a FCRA-articulated purpose, it is not considered a consumer report.

State regulation is possible in circumstances where the report is used for purposes outside the FCRA definition, such as: screening a volunteer, evaluating a possible companion (dating), satisfying curiosity about a neighbor, researching a witness or litigant, learning about a potential business partner, finding people, learning about witnesses who will testify in court, preventing fraud, assisting law enforcement in locating people or for other law enforcement-related purposes, or to conduct a private investigation. Further, FCRA leaves open for state regulation circumstances in which records are collected directly by the person who is going to use them. For example, if a landlord does her own criminal background check using the public records available on the Minnesota Bureau of Criminal Apprehension website, FCRA does not apply and state regulation is possible.[35] Likewise, since there is nothing in FCRA that limits how information is collected and made available through the media, the state may regulate circumstances where a blogger (commonly considered "media") disseminates mined government data.

3. **When no adverse action is taken.** The FCRA definition of an adverse action is, for purposes of this report,

    - A denial of employment or any other decision that negatively affects a current employee; or
    - A decision made or action taken in a transaction started by the consumer that is not in the interests of the consumer.(15 U.S.C. section 1681a(k))

[35] FTC staff has determined that public records sources, like criminal justice agencies, are not "consumer reporting agencies." The FTC reached this conclusion, in part, because access to public records is governed by state or federal access laws and these requirements compete with some of the provisions of FCRA. See FTC Staff Opinion *Brinckerhoff-Goeke* dated June 9, 1998, viewed online July 3, 2008 at www.ftc.gov/os/statutes/fcra/goeke.shtm

This definition has been interpreted as covering decisions made by landlords about individuals applying to rental housing.[36] Though it takes adverse action to trigger FCRA rights, in many situations it may not be apparent nor be clear that an adverse action has occurred (see diagram in Appendix D: *Lease or employment applicants' rights to notice under the Fair Credit Reporting Act, and their opportunities to seek remedy*). Consider the following examples:

- A landlord receives a large number of applications for her vacant apartment. She obtains consumer reports on all of the applicants. The first applicant doesn't meet her income requirements. The second applicant in the pile appears to have an arrest that troubles the landlord. She sets the application aside. The third applicant meets the income requirements, doesn't have a criminal record and so the apartment is offered to that person. Is this an adverse action that would cause the second applicant to get the notices required by FCRA?

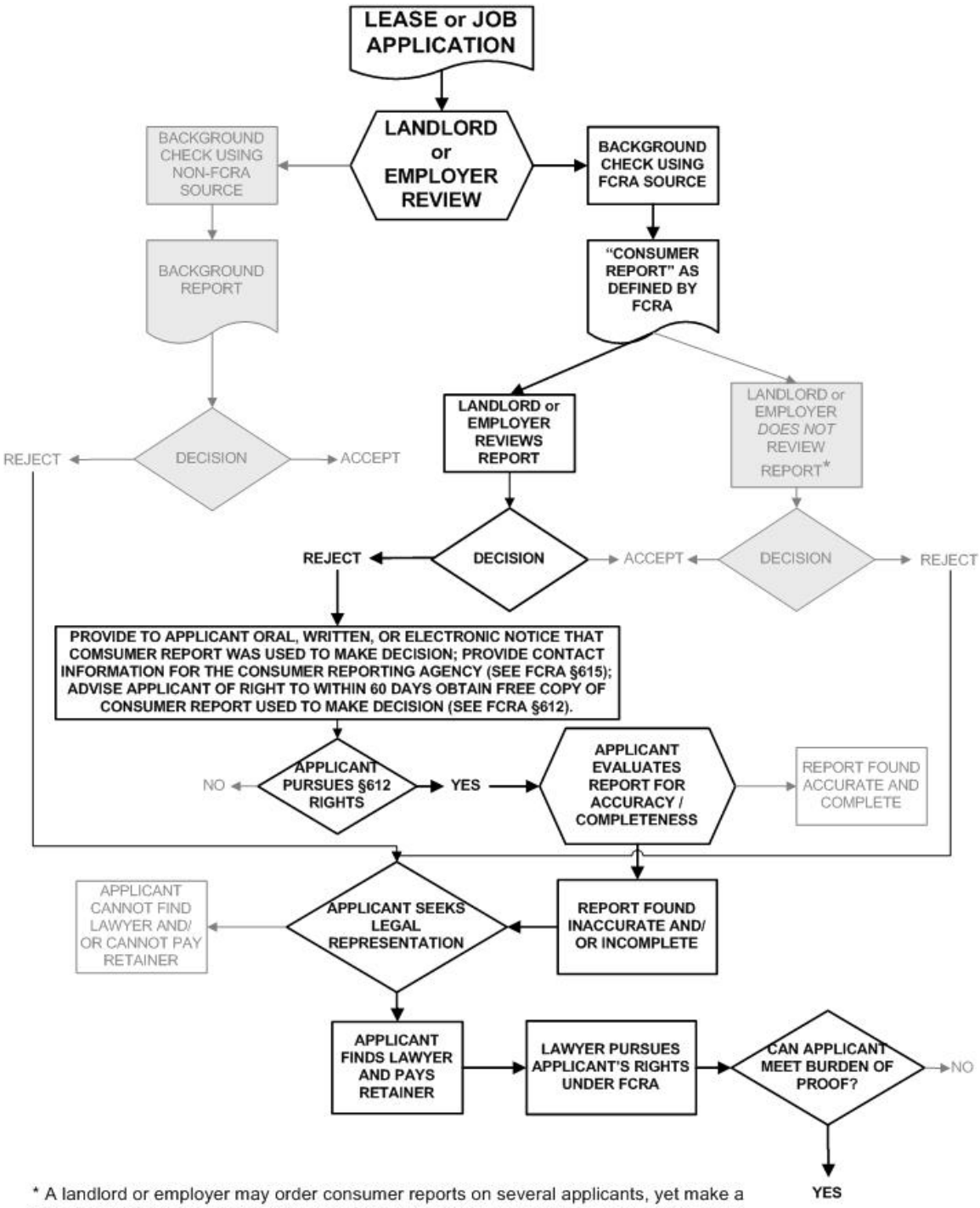
- An employer gets consumer reports on all five finalists for the position. The first finalist meets all the requirements and is offered the job and the remaining four consumer reports are never reviewed. Is this an adverse action?

[36] See FTC Staff Opinion *Haynes-Riddle* dated March 17, 1999 viewed online July 3, 2008 at www.ftc.gov/os/statutes/fcra/riddle.shtm

Appendix C

DATA MINING DELIVERY TEAM

Lease or employment applicants' rights to notice under the Fair Credit Reporting Act, and their opportunites to seek remedy



* A landlord or employer may order consumer reports on several applicants, yet make a decision to accept another applicant before reviewing every consumer report they have ordered.

Shaded boxes denote those events likely to be invisible to data subject

Appendix D

Working document used by delivery team to identify approaches

Criminal and Juvenile Justice Information Task Force, Data Mining Delivery Team
Summary of member assessment of approaches, May 14, 2008

Note: Assessments are not formal votes; all approaches are still open to discussion
KEY
☑= would like to recommend to the Task Force and Policy Group
☐= would recommend, but with caution (a concern you would like to discuss)
☒ = would not recommend

Approach	Implementation ideas	Members' assessment	Examples and precedent
1. Limiting information available / remove "staleness"	**1A**. Develop rules regarding the useful life of a criminal justice system record (e.g., useful life of misdemeanor arrest is less than felony conviction). Classify expired records as not public.	☑☑☑☑ ☑☑ ☒	▪ **California:** consumer reporting agency may not report convictions over 7 years old; see [cite]; background checks for school district employees shall not include records of criminal proceedings that did not result in conviction, see Cal.Educ.Code Title 2, Div. 3, Part 25, Ch. 5, Art. 1§ 45125(b)(1); further, it is forbidden to ask job applicants about arrests not leading to conviction, sealed or expunged convictions, or successfully completed pretrial diversions; see Cal. Code of Regulations, Title 2, Div. 4, Ch.2, Subch. 2 §7287.4 (d)(1)(A-C). ▪ **Montana:** consumer reporting agency may not report arrests or convictions over 7 years old; see Mont.Code Ann. 31-3-112, "Obsolete information" (2007). ▪ **Nevada:** consumer reporting agency may not report convictions over 7 years old; see NRS 598C.150. ▪ **New Mexico:** consumer reporting agency may not report convictions over 7 years old. see NM Statute 56-3-6.
	1B. Limit commercial users' access to arrest / booking data unless conviction has occurred	☑☑☑ ☐☐ ☒☒	▪ **Los Angeles** Police Department declines to provide arrestee addresses to commercial services; though challenged on 1st amendment free-speech grounds, the restriction was upheld by US Supreme Court in LAPD v. United Reporting , 528 U.S. 32 (1999). ▪ **Connecticut:** Nonconviction information may be disclosed only to (1.) state and federal criminal justice agencies; (2.) agencies and persons which require such information to implement a statute or executive order that expressly refers to criminal conduct; (3.) agencies or persons authorized by a court order, statute or decisional law to receive criminal history record information. Further, Connecticut law provides that dissemination of nonconviction information to noncriminal justice agencies shall (1.) be used by such agencies only for the purpose for which it was given and shall not be redisseminated; and, (2.) No agency or individual shall confirm the existence or nonexistence of nonconviction information to any person or agency that would not be eligible to receive the information itself. See GSC Title 54,

			Chapter 961a Sec. 54-142n and Sec. 54-142o Criminal Records: Sec. 54-142n.
	1C. When court disposition data later changes status due to court order, earlier mined data miner's records should conform to the court order.	☑☑☑☑ ☐☐	For example, when a court record is mined and later there is an expungement or a dismissal following a continuance for dismissal, use of the earlier-mined data should conform to the order. ▪ **Montana:** for an example of a statute that fails to consider earlier-mined data, see Mont. Code Ann. 46-18-204 (2007): after dismissal following deferred imposition of sentence, all records and data relating to the charge are confidential and public access may be obtained only by court order. "Public access" likely means access from the court itself, not public access from a data miner.
2. Regulating data miners / systems	**2A.** Require data miners to update their data so that they do not disseminate records that have converted to not public.	☑☑☑☑ ☑☑	▪ **Minnesota:** Senate files 914/3235 (pending in 08 Legislative session) would require business screening services to update their data from the source monthly ▪ **Connecticut:** Public Act 07-243 requires background screening services to update their data at the time they provide it to the data customer.
	2B. Certify and train commercial users of criminal justice data	☑ ☐☐☐☐	▪ **Massachusetts:** Exec. Order 495 requires entities accessing data to be certified, and receive training to maintain certification.
	C. Allow the market to self-regulate	☒☒☒☒ ☒☒	
3. Fair Information Practice Principles	Require those who use background reports that contain criminal justice data to provide notice and access to data subjects.	☑☑☑☑ ☐ ☒	▪ **Minnesota:** Applies some FIPPs to the private sector; see, e.g., MS§325E.61 (security breach notification). ▪ **Minneapolis and St. Paul:** Ordinances require landlords who take application fees to give lease applicants reasons for rejection, criteria used, and contact information for the data miner utilized, see St. Paul City Code §54.03; Minneapolis Code of Ordinances §244.1919(16)(c). ▪ **Wisconsin:** Fair Employment law forbids employers from firing or refusing to hire due to arrests or convictions not substantially related to circumstances of the person's job; see Wisconsin Statutes. 111.31-111.395. ▪ **California**: Online Privacy Protection Act requires commercial web sites and online services collecting personal data to post and comply with privacy policy; see California Business and Professions Code, § 22575-22579 Further, California's "FCRA Plus" statute gives data subjects greater rights to see the results of background checks, increasing the chance that incomplete or inaccurate information can be corrected. California FCRA-Plus gives data subjects rights when affected by data miners not covered by federal FCRA, such as web sites offering to find "anything out about anybody." See California Civil Code §1786.

4. Improve accuracy of records	**4A.** Ensure that records held by data miners accurately reflect the state of records at the government source	☑☑☑☑☑☑	▪ **Minnesota**: Data Practices Conference Committee has approved language (would be effective 7-1-09 if passed and signed) that would require businesses disseminating criminal record information unless the data has been updated within the previous month. MN Senate file 3235 (2008); this is the record-refresh idea set forth in #1C above.
	4B. Provide increased ability for individuals to access and correct records at the source.	☑☑☑☑☑☑	▪ **Minnesota**: provides data subjects with the opportunity to view data accessible through the BCA's Integrated Search Service, see MS§13.873. Minnesota's Data Practices Act requires that data subjects be given access to government data (MS§13.04), be notified of their right to access data (MS§13.05, Subd. 8), and be able to challenge data that are not accurate or are incomplete (MS§13.04).
5. Remedies for individuals who are impacted by the system	**5A.** Limit private employers' ability to inquire about or to use arrest or conviction history to fire or refuse to hire; e.g., could expand current Criminal Offender Rehabilitation Act so it applies to private sector.	☑☑☐☐☐☐	▪ **Arizona:** Civil Rights law limits an employer's inquiry of an applicant regarding prior convictions. The employer must include a statement that a conviction will not be an absolute bar to employment. See http://www.azag.gov/civil_rights/PreEmploymentInquiriesGuide.pdf. ▪ **California:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Cal. Civ Code 1786.18(a)(7). ▪ **Florida:** limits data dissemination by charging for records. There is no bulk discount for criminal record data. Therefore, for a commercial vendor wishing to purchase the roughly 13 million records held by the Florida Department of Law Enforcement (FDLE) would need to pay the State's standard $23 per search charge. See Florida Department of Law Enforcement, "Obtaining Criminal History Information," available at **www.fdle.state.fl.us/criminalhistory.** ▪ **Georgia:** If an employment decision is made adverse to a person whose record was obtained pursuant to this Code section, the person will be informed by the business or person making the adverse employment decision of all information pertinent to that decision. This disclosure shall include information that a record was obtained from the center, the specific contents of the record, and the effect the record had upon the decision. Failure to provide all such information to the person subject to the adverse decision shall be a misdemeanor. See GA Code 35-3-34 (3) (b). ▪ **Hawaii:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see [cite]; further, employers can consider only rationally-related occurring in past 10 years, and then only after conditional offer of employment. Haw. Rev . Stat 378-2.5.

5A, continued

- **Illinois:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see 775 ILCS 5/2-103.
- **Kansas:** If it is to disqualify a job applicant [or employee?], a conviction must reasonably relate to trustworthiness or safety/wellbeing of coworkers/customers; see http://www.khrc.net/hiring.html#EMPLOYMENT%20INQUIRY Kansas Statutes 50-704. Obsolete information. (a) Except as authorized under subsection (b) of this section, no consumer reporting agency may make any consumer report containing any of the following items of information: (5) records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years; and (6) any other adverse item of information which antedates the report by more than seven years.
- **Kentucky:** No consumer reporting agency shall maintain any information in its files relating to any charge in any Kentucky criminal case unless the charge has resulted in a conviction. See KRS Chapter 367.00 §310.
- **Massachusetts:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Mass Gen, Laws ch. 151B 4(9)(ii).
- **Michigan:** Public and private employers and occupational licensing agencies cannot use arrests that never lead to conviction; See Michigan Complied Laws Act 453 of 1976 37.2205a (1) – "Convictions: An employer, employment agency, or labor organization, other than a law enforcement agency of this state or a political subdivision of this state, shall not in connection with the terms, conditions, or privileges of employment or membership request, make or maintain a record of information regarding a misdemeanor arrest, detention, or disposition where a conviction did not result. A person is not guilty of perjury or otherwise for giving a false statement by failing to recite or acknowledge information the person has a civil right to withhold by this section. This section does not apply to information relative to a felony charge before conviction or dismissal."
- **Minnesota:** Criminal Offenders Rehabilitation Act provides that no one shall be disqualified from public employment or denied license solely because of a conviction not directly related to the employment; see MS§364.
- **New Mexico:** A credit bureau may report the following matters for no longer than the specified periods: arrests and indictments pending trial, or convictions of crimes for not longer than seven years from date of release or parole. Such items shall no longer be reported if at any time it learned that after a conviction a full pardon has been granted, or after an arrest or indictment a conviction did not result; and any other data not otherwise specified in this section, for not longer than seven years. See New Mexico Statute Chapter 56-3-6(a)(5).

5A, continued

- **New York:** Public and private employers and occupational licensing agencies cannot use arrests never leading to

conviction; see [cite]; further, public and private employers prohibited from having blanket policy denying employment to former offenders; see [cite]; further, employers must determine that there is a direct relationship between conviction history and the job's specific duties and whether unreasonable risk would be created if the person is hired. New York State Consolidated Laws Article 25 Section 380-j – Prohibited Information Prohibited information. (a) No consumer reporting agency shall report or maintain in the file on a consumer, information: (1) relative to an arrest or a criminal charge unless there has been a criminal conviction for such offense, or unless such charges are still pending. (f) (1) Except as authorized under paragraph two of this subdivision, no consumer reporting agency may make any consumer report containing any of the following items of information. (V) records of conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years.

- **Ohio:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Ohio Civil Rights Commission's "A guide for Application Forms and Interviews".
- **Rhode Island:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Rhode Island Gen. Laws. 28-5-7(7).
- **Utah:** Public and private employers and occupational licensing agencies cannot use arrests never leading to conviction; see Utah Industrial Commission Anti-Discrimination Division, Pre-employment Inquiry Guide.
- **Washington:** Records of arrest, indictments, or conviction of crime older than 7 years from the date of disposition, release, or parole date dissemination prohibited. RCW 19.182.040.
- **Wisconsin:** Fair Employment law prohibits firing or disqualification from employment because of arrest or conviction unless the arrest or conviction is substantially related to the employment. See Wisconsin Fair Employment Law, Wisconsin Statutes. 111.31-111.395 or, for more specific information, http://dwd.wisconsin.gov/er/discrimination_civil_rights/fair_employment_law.htm.

5B. Add arrest and/or conviction status to list of protected classes under human rights law. ☑ ☐ ☒☒☒☒

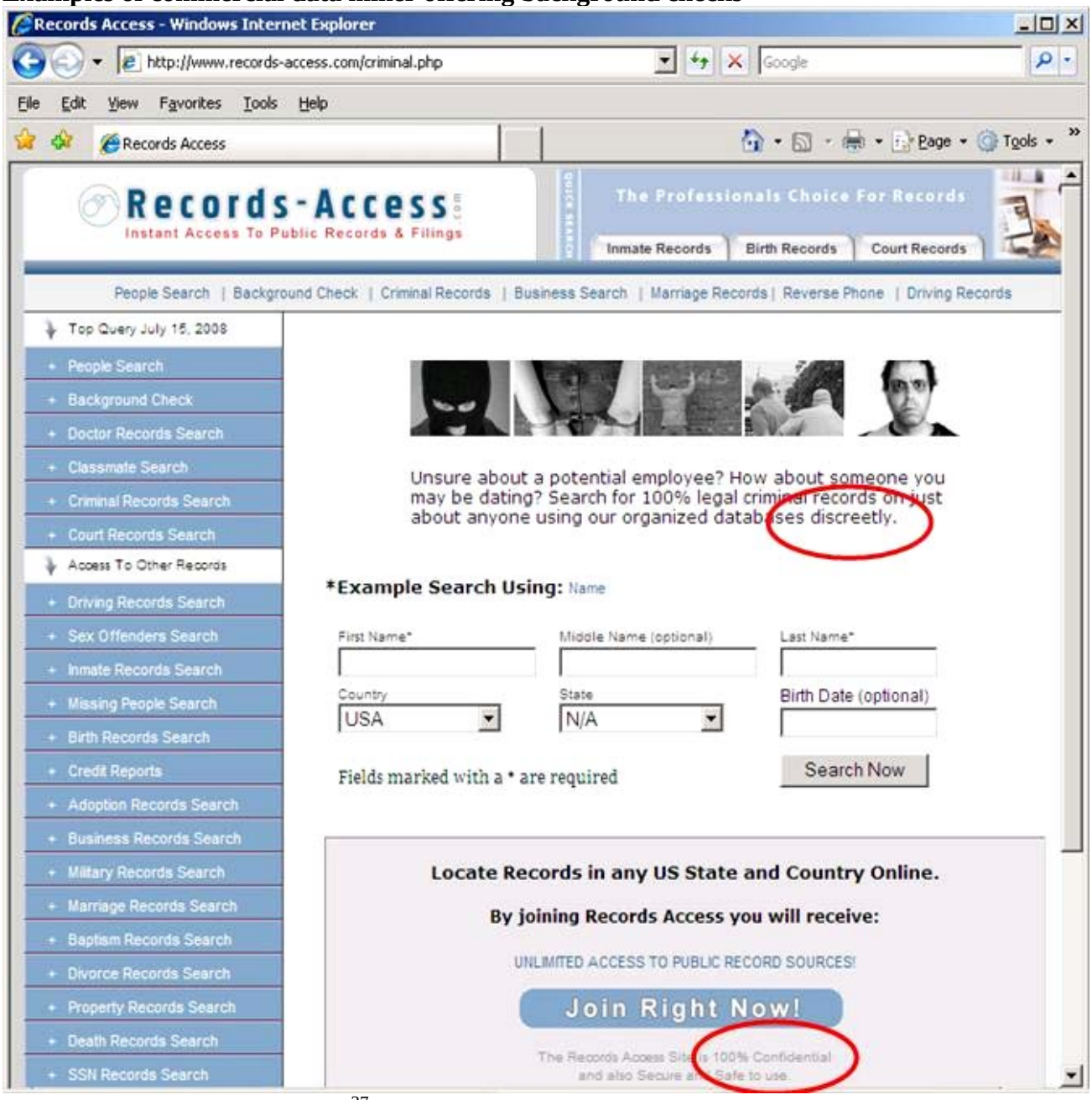
- **Colorado:** Civil Rights Commission limits employer's questions of an applicant, and any questions in this area may lead to discriminatory inference. Employers can inquire about actual convictions which are substantially related to applicant's ability to perform a specific job if this question is addressed to every applicant. http://www.dora.state.co.us/civil-rights/Publications/JobDiscrim2001.pdf Further, no consumer reporting agency is allowed make any consumer report containing records of arrest, indictment or conviction of a crime that, from the date of disposition, release, or parole, predate the report by more than seven years. See CRS 12-14-.3-105.3 (1)(e).

5C. Create enforcement ☑

	mechanism allowing attorney general to enforce compliance.	☐☐☐ ☒	
	5D. Create right of action allowing civil complaint by those injured by statutory noncompliance.	☑ ☐☐ ☒☒	
6. Education	Task (& fund) state agency with the duty to educate data consumers, data subjects and government agencies about obligations and rights under state law	☑☑☑☑ ☑☑	▪ **California:** Created an Office of Information Security and Privacy Protection in 2000 whose mission is to identify consumer problems in the privacy area and encourage the development of fair information practices. See http://www.oispp.ca.gov/. ▪ As with California, one approach is to create state agency to register data miners, serve in an ombuds capacity, and coordinate record changes like expungements and sealing records. To ensure meaningful access and other Fair Information Practice Principles, there must be a way to provide notice or for a subject to learn about all the data mining companies that collect their information. Any company engaged in the collection, maintenance, and/or sale of personally identifiable information could be required to register with an agency in Minnesota designated by the Legislature. The agency could be called something like the Minnesota Office of Information Security and Privacy Protection. The agency could coordinate transmittal of sealing / expungement orders from the courts to registered data miners. Data miners could also be required to disclose the types of businesses and entities to whom they disclose personal information to as well as to disclose the safeguards they have in place for verifying those entities that received the data. ▪ A state data privacy / consumer protection agency could be charged with educating individuals, consumers and businesses on privacy rights and regulations in Minnesota. As part of any enforcement action, individuals or the privacy agency should be able to obtain by court order an audit of a commercial data broker, data administrator, or data miner.

Appendix E

Examples of commercial data miner offering background checks



See also the following examples[37]:

1. http://www.backgroundrecordsregistry.com/
2. http://www.discreetresearch.com/
3. http://www.easybackgroundchecks.com/
4. http://www.efindoutthetruth.com/
5. http://www.instant-background-check.com/
6. http://www.netdetective.com/
7. https://www.criminalrecordreporter.com/
8. http://www.instantbackgroundreport.com/
9. http://www.integrascan.com/
10. http://www.usarecordssearch.com/
11. http://www.criminal-records.us.com/
12. http://www.screensafecheck.com/
13. http://www.efindoutthetruth.com/
14. http://www.whoishe.com/
15. http://www.a1peoplesearch.com
16. http://www.netsleuth.com

[37] No web site listed here, when viewed online July 23, 2008, contained any reference to FCRA on its main page.