DATA REPLICATION REPORT

TASK FORCE RECOMMENDATIONS TO THE PUBLIC ACCESS COMMITTEE

MARCH 2012

Table of Contents

Data Replication Report

Introduction

Pursuant to Chief Justice Directive 05-01, the Judicial Department does not release bulk data from its electronic court case management system (CMS). This includes replicating the entire Judicial Department court records database. State Legislators and third party vendors requested that the Judicial Department review that policy. This report is focused on database replication only and does not address aggregate or composite data releases.

Therefore, in August 2011 a Task Force was commissioned to research historical bulk data release reasoning, technology, benefits and detriments; and to review the current policy related to bulk data releases using a form of data replication. The Task Force was also asked to examine the advantages and disadvantages of the process and provide recommendations to the Public Access Committee regarding this policy decision.

The Task Force Members are as follows:

Chad Cornelius, Task Force Chair, CIO for Colorado State Judicial
Larry Webster, National Center for State Courts (Consultant)
Jerry Marroney, Colorado State Court Administrator
Sherry Stwalley, Director of Planning & Analysis and Judicial's Legislative Liaison
Chief Judge William Sylvester, 18th Judicial District
Mary Perry, District Administrator, 4th Judicial District
Christopher Ryan, Clerk of the Supreme Court and Court of Appeals
Amber Roth, Clerk of Court, Jefferson Combined Courts
Ron Ozga, IT Director at State of Colorado, Governor's Office of Information Technology
Linda Bowers, Court Services Manager for the Colorado Judicial Department

The Task Force met during the fall of 2011 and reviewed the history and purpose of the current record access policy. They considered whether the current access to electronic court records is suitable. This included weighing factors such as government transparency, access to records, parties' privacy, accurate and updated information, and any other applicable matter related to the Judicial Department's records and data replication.

Access History and Policy Evolution

The Judicial Department began collecting electronic information in an electronic CMS in 1978. Only the large metropolitan courts stored information in this system until the mid-1990s when the Judicial Department began implementing the CMS statewide. By January 1996 all state courts were entering court records into the electronic CMS.

In the early-1990s private companies began expressing interest in obtaining access to the electronic records to use commercially. Without a policy to address this new technology, data releases of the Judicial Department's statewide trial court database was released to private vendors. Creating the tapes that were ultimately released took two to three weeks to compile. Once a vendor received the tapes,

they had to program the data to display in their program. This meant that the data being displayed and available on the Internet was at least three weeks old (and frequently older) by the time it was available. Additionally, these tape releases were only created on a quarterly basis when staff was available to create them.

In 1997, parties and court staff reported concerns to the State Court Administrator's Office (SCA) regarding inaccurate and confidential information that was available on the Internet. Though the Judicial Department attempted to remove confidential information from the data releases, the SCA learned that some trial court minute orders contained confidential information such as sex offender victims' names, children's names and other confidential information. Because of the case management system's constraints and the limited method in which data could be entered, confidential addresses, driver's license numbers and social security numbers were inadvertently being released. Additionally, as cases were sealed by the court, there was no way to remove them from the data releases that had previously been distributed. Due to the length of time it took to create and disseminate the tape containing data releases and the extended time between data releases, information regarding protection orders and warrants was also inaccurate and outdated.

Once vendors received data releases, they were left to their own devices to determine how to program and display the court records. There were no data entry standards at the time; therefore the information contained in the Judicial Department's database was not easily deciphered. Records were not only being displayed by the commercial entities that received the data releases directly from the Judicial Department, but the vendors also sold the data to other companies/subscribers—some of which were outside of the United States. There was no way to identify these commercial entities to get records corrected or removed from the Internet when/if they should no longer be displaying. Many of these vendors did not receive the data as often, some of them only updating their records on a yearly basis. Yet, employers were using this information to make personnel decisions.

The SCA attempted to create programming that would cleanse all of the tables and fields to remove confidential information. However, a satisfactory solution could not be identified; therefore the data releases were discontinued in 1997. This prompted a vendor to file a lawsuit that would require the SCA to continue the data releases. In September 1997, the District Court ordered the Judicial Department to continue to provide the data. Appeals were filed and in November 1999 the Colorado Supreme Court ruled that the Judicial Department was not required to manipulate data solely for purposes of disclosure and that the courts themselves retain authority over the dissemination of court records[1].

A Public Access Committee was created in May 1998 to adopt policies to govern release of court records as authorized by Chief Justice Directive 98-05. The Committee issued its first data access policies in October 1998. Additionally, the Judicial Department began to work on an RFP that would allow the Department to select a vendor that would create real-time electronic access to court records so that the records being displayed on the Internet would be updated and remain accurate. The RFP was awarded in April 2000. Upon awarding the project, a vendor acted as the Judicial Department's agent[2] to provide public access. Technology limitations and a desire to keep vendors competitive compelled the Department to allow this agent to replicate the data to additional vendors. However, issues continued

[1] *Office of the State Court Administrator v. Background Information Services, Inc*., 994 P.2d 420 (Colo. 1999)

[2] As an agent for a government agency, a vendor provides the services that the agency does not have resources to internally provide. This relationship was substantiated by contract. Acting as the Department's agent, this vendor had access to all necessary data that was needed to provide these services.

to surface regarding court records being posted on the Internet that were not updated in the real-time format that was required by contract.

A second RFP was issued in November 2004 because the vendor contract was approaching expiration. This RFP was similar to the first except that the successful vendor was required to provide real-time XML access for other vendors rather than replicating the entire database. Using this methodology, records would be available in real-time on a name-by-name or case-by-case basis rather than allowing the entire database to be stored on multiple servers. This was to address the issue of stale data being made available on the Internet and the database being sold to commercial entities that were not contracted with the Department. Additionally, the successful vendor was required to provide free access to approved government agencies. The agent also created additional levels of access so that government agencies could have access to non-public court records as allowed by statute.

Advances in technology have allowed the Judicial Department to assume the task of providing public and government agency access. In July 2010, when the contract with the Department's previous agent expired, the Judicial Department began offering real-time access to court records both to vendors and approved government agencies. This is the same access as the previous vendor/agent provided since January 2006. All access to the court records are in a real-time search, either by party name or by case number.

Other Colorado State Government Data Access

Participants of this Task Force researched but could not identify any other Colorado State Government Agency that replicates its database to vendors. There are a few agencies (such as Department of Revenue (DOR) and the Department of Motor Vehicle (DMV) that provide limited information, but not complete databases replicated to vendors. There are some Executive Branch agencies that provide name searches of their databases; most charge a fee for this service.

The Executive Branch is also in the process of reviewing its data sharing policies. At this time, data sharing in the Executive Branch is focused on interagency sharing rather than access by the public or commercial entities. An Advisory Board, the Government Data Advisory Board (GDAB), was formed to review State policy and data access. The GDAB was created by the legislature in 2009 and is a multi-agency central governance authority, comprised of representatives of 12 state agencies, local governments, non-governmental organizations and research institutes, and a wide variety of education stakeholders. The GDAB's mission is to provide guidance and recommendations on how the state should govern and manage data and data management systems to improve the efficiency and effectiveness of state government, citizen service delivery and policy-making. The GDAB is a unique Board with very few like it in any other state in the country, established in legislation and appointed by the Governor, to provide the central governing structure for enterprise data sharing initiatives.[3]

This is the State's first enterprise data strategy. The work being done is to strategically focus on providing long term and scalable solutions. There is a danger in trying to do too much with limited resources, and conversely in not getting enough accomplished to show value, commitment, and progress. Necessarily, efforts will be undertaken in a modular approach, and prioritized appropriately.

[3] Government Data Advisory Board website: http://www.colorado.gov/cs/Satellite/OIT-EADG/CBON/1251579896288

Certainly, the State must deal responsibly with its existing, sometimes aging, infrastructure, and agencies do not have the human capital to move as quickly as perhaps some would wish.

Other States' Judicial Records Access

Colorado is on the cutting edge of technology boasting a statewide court case management system that integrates court records with probation, financial, Colorado Integrated Criminal Justice Information System (CICJIS), Department of Human Services, and e-filing programs. This comprehensive system is unique in the quantity of data that is collected and maintained. Many states have separate case management systems in every county or in regions of the state. It is common for states to provide composite data releases; however, staff that researched the various states' systems were unable to identify another state that replicated their database to vendors. Many states did not provide any real-time access to their records except for a judicial department maintained website. These sites generally provided information on a name-by-name or case-by-case basis.

Listed below are examples of representative states' policies:

New Mexico Judicial Branch Release Policy

Release of Electronic Court Records Policy August 20, 2004: The New Mexico Judiciary strongly supports the concept of open government and public access to official records. At the same time the judiciary recognizes its obligations to protect the privacy interests of those who deal with the judiciary.

The purpose of this policy is to provide guidance to staff who must respond to requests for court records in either electronic or paper form. Because of the fast-changing nature of technologies associated with the storage, capture, retrieval and distribution of court records this policy must be frequently modified to adapt to a changing technical environment. All requests that do not clearly fall within the guidelines outlined in this policy must be referred to the Administrative Authority for the Administrative Office of the Courts (AOC). The JIFFY Public Access Committee and the AOC General Counsel will assist the Administrative Authority in making determinations regarding such requests.

I. Requests from for-profit data consolidators and re-sellers: No bulk records will be sold to organizations that gather data from public sources and then subsequently resell such data since once bulk data is provided to bulk resellers it cannot be quality controlled, expunged, sealed or amended.
II. Requests from public organizations, private organizations or individuals:

Such written requests shall receive a written response within 3 working days.

The following types of requests shall be denied:

- Requests for confidential, privileged and proprietary data or any other data that is prevented by statute or court order from being released
- Requests that will be burdensome or hamper the operations of the court
- Requests for information that is not collected or retained, or is collected in a statistically invalid manner

- Requests for information in a format that is not maintained
- Requests for electronic information where the official record is not electronic and the electronic record is not accurate representation of the official record or Requests related to security information protected by NMSA 1978, Section 14-2-1(A)(8) (2003).

All denied written requests shall be forwarded to the Administrative Authority for the AOC for possible further consideration. Under certain circumstances the Administrative Authority may determine that release of requested information, in part or in total, is appropriate under the Inspection of Public Records Act but that further publication of such information should be restricted for the public welfare.

JID staff shall work with requestors of electronic information to clearly define data requests to minimize impact on judicial operations. For example, assistance might be provided in defining query parameters such as case type, event type, charge category, date constraints and specific data fields needed. Also, assistance can be provided in defining queries to exclude confidential and proprietary data.

Data can be provided on media such as streaming tape, CD, DVD, magnetic diskette, or even on paper, as long as there is a reasonable capability to deliver data on the requested media. Requestors will be charged for all actual costs of generating queries, including but not limited to costs for materials and staff time. A written estimate shall be provided to the requestor before queries are executed.

Requests for direct links to court databases: Direct links have the potential to disrupt operational electronic records processing and thus hamper delivery of court services. In addition, it is difficult to provide adequate quality control for unlimited, uncontrolled ad hoc queries. Finally, such links also present significant security challenges, even when secure access methods are used.

Therefore, absent exceptional circumstances and JIFFY approval, requests for direct links to court databases shall be denied.

Utah Electronic Court Record Release Policy

Rule 4-202.02. Records classification.

Statement of the Rule:

(1) Court records are public unless otherwise classified by this rule.[4]

(2) Public court records include but are not limited to:

(2)(A) abstract of a citation that redacts all non-public information;

(2)(B) aggregate records without non-public information and without personal identifying information;

(2)(C) arrest warrants, but a court may restrict access before service;

(2)(D) audit reports;

(2)(E) case files;

[4] Any person may access a public court record. Utah Court Rule 4-202.03(1).

(2)(F) committee reports after release by the Judicial Council or the court that requested the study;
(2)(G) contracts entered into by the judicial branch and records of compliance with the terms of a contract;
(2)(H) drafts that were never finalized but were relied upon in carrying out an action or policy;
(2)(I) exhibits, but the judge may regulate or deny access to ensure the integrity of the exhibit, a fair trial or interests favoring closure;
(2)(J) financial records;
(2)(K) indexes approved by the Management Committee of the Judicial Council, including the following, in courts other than the juvenile court; an index may contain any other index information:
(2)(K)(i) amount in controversy;
(2)(K)(ii) attorney name;
(2)(K)(iii) case number;
(2)(K)(iv) case status;
(2)(K)(v) civil case type or criminal violation;
(2)(K)(vi) civil judgment or criminal disposition;
(2)(K)(vii) daily calendar;
(2)(K)(viii) file date;
(2)(K)(ix) party name;
(2)(L) name, business address, business telephone number, and business email address of an adult person or business entity other than a party, but the name of a juror or prospective juror is private until released by the judge;
(2)(M) name, address, telephone number, email address, date of birth, and last four digits of the following: driver's license number; social security number; or account number of a party;
(2)(N) name, business address, business telephone number, and business email address of a lawyer appearing in a case;
(2)(O) name, business address, business telephone number, and business email address of court personnel other than judges;
(2)(P) name, business address, and business telephone number of judges;
(2)(Q) name, gender, gross salary and benefits, job title and description, number of hours worked per pay period, dates of employment, and relevant qualifications of a current or former court personnel;
(2)(R) opinions, including concurring and dissenting opinions, and orders entered in open hearings;
(2)(S) order or decision classifying a record as not public;
(2)(T) private record if the subject of the record has given written permission to make the record public;
(2)(U) publications of the administrative office of the courts;
(2)(V) record in which the judicial branch determines or states an opinion on the rights of the state, a political subdivision, the public, or a person;
(2)(W) record of the receipt or expenditure of public funds;
(2)(X) record or minutes of an open meeting or hearing and the transcript of them;
(2)(Y) record of formal discipline of current or former court personnel or of a person regulated by the judicial branch if the disciplinary action has been

completed, and all time periods for administrative appeal have expired, and the disciplinary action was sustained;

(2)(Z) record of a request for a record;

(2)(AA) reports used by the judiciary if all of the data in the report is public or the Judicial Council designates the report as a public record;

(2)(BB) rules of the Supreme Court and Judicial Council;

(2)(CC) search warrants, the application and all affidavits or other recorded testimony on which a warrant is based are public after they are unsealed under Utah Rule of Criminal Procedure 40;

(2)(DD) statistical data derived from public and non-public records but that disclose only public data;

(2)(EE) Notwithstanding subsections (6) and (7), if a petition, indictment, or information is filed charging a person 14 years of age or older with a felony or an offense that would be a felony if committed by an adult, the petition, indictment or information, the adjudication order, the disposition order, and the delinquency history summary of the person are public records. The delinquency history summary shall contain the name of the person, a listing of the offenses for which the person was adjudged to be within the jurisdiction of the juvenile court, and the disposition of the court in each of those offenses.

(3) The following court records are sealed:[5]

(3)(A) adoption records, which are private until sealed;

(3)(B) expunged records;

(3)(C) orders authorizing installation of pen register or trap and trace device under Utah Code Section 77-23a-15;

(3)(D) records showing the identity of a confidential informant;

(3)(E) records relating to the possession of a financial institution by the commissioner of financial institutions under Utah Code Section 7-2-6;

(3)(F) wills deposited for safe keeping under Utah Code Section 75-2-901;

(3)(G) records designated as sealed by rule of the Supreme Court;

(3)(H) record of a Children's Justice Center investigative interview after the conclusion of any legal proceedings; and

(3)(I) other records as ordered by the court under Rule 4-202.04.

(4) The following court records are private:[6]

(4)(A) adoption records until sealed;

---

[5] An adoptive parent or adult adoptee may obtain a certified copy of the adoption decree upon request and presentation of positive identification. Otherwise, no one may access a sealed court record except by order of the court. A judge may review a sealed record when the circumstances warrant. Utah Court Rule 4-202.01(2).

[6] (3) The following may access a private court record: (3)(A) the subject of the record; (3)(B) the attorney for the subject of the record or an individual who has a power of attorney from the subject of the record; (3)(C) the parent or guardian of the subject of the record if the subject is an unemancipated minor or under a legal incapacity; (3)(D) a person with a notarized release from the subject of the record or the subject's legal representative dated no more than 90 days before the date the request is made; (3)(E) a party or attorney for a party to litigation in which the record is filed; (3)(F) an interested person to an action under the Uniform Probate Code; (3)(G) the person who submitted the record; (3)(H) anyone by court order; (3)(I) court personnel, but only to achieve the purpose for which the record was submitted; (3)(J) a person provided the record under Rule 4-202.04 or Rule 4-202.05; and (3)(K) a governmental entity with which the record is shared under Rule 4-202.10. Utah Court Rule 4-202.01(3).

(4)(B) aggregate records other than public aggregate records under subsection (2);
(4)(C) alternative dispute resolution records;
(4)(D) applications for accommodation under the Americans with Disabilities Act;
(4)(E) citation, but an abstract of a citation that redacts all non-public information is public;
(4)(F) custody evaluations;
(4)(G) eligibility for benefits or services or the determination of the benefit level;
(4)(H) home studies;
(4)(I) judgment information statement;
(4)(J) judicial review of final agency action under Utah Code Section 62A-4a-1009;
(4)(K) the following personal identifying information about a party: driver's license number, social security number, account description and number, password, identification number, maiden name and mother's maiden name, and similar personal identifying information;
(4)(L) the following personal identifying information about a person other than a party: residential address, personal email address, personal telephone number; date of birth, driver's license number, social security number, account description and number, password, identification number, maiden name, mother's maiden name, and similar personal identifying information;
(4)(M) guardianship cases and conservatorship cases, except the order of appointment and letter of appointment, which are public;
(4)(N) medical, psychiatric, or psychological records;
(4)(O) name of a minor, except that the name of a minor party is public in the following district and justice court proceedings:
(4)(O)(i) name change of a minor;
(4)(O)(ii) guardianship or conservatorship for a minor; and
(4)(O)(iii) felony, misdemeanor or infraction;
(4)(P) personnel file of a current or former court personnel or applicant for employment;
(4)(Q) photograph, film or video of a crime victim or of the petitioner in a cohabitant abuse action or civil stalking action;
(4)(R) presentence investigation report;
(4)(S) record classified as private or controlled by a governmental entity and shared with the court under the Government Records Access and Management Act;
(4)(T) non-public record provided by a governmental entity of a state or the United States;
(4)(U) record regarding the character or competence of an individual;
(4)(V) record containing information the disclosure of which constitutes an unwarranted invasion of personal privacy;
(4)(W) record involving the commitment of a person under Title 62A, Chapter 15, Substance Abuse and Mental Health Act;
(4)(X) record of a court hearing closed to the public or of a child's testimony taken under URCrP 15.5:
(4)(X)(i) permanently if the hearing is not traditionally open to the public and public access does not play a significant positive role in the process; or
(4)(X)(ii) if the hearing is traditionally open to the public, until the judge determines it is possible to release the record without prejudice to the interests that justified the closure;

(4)(Y) record of a delinquency proceeding against an insurer under Utah Code Section 31a-27-203;
(4)(Z) record submitted by a senior judge or court commissioner regarding performance evaluation and certification;
(4)(AA) record submitted for in camera review until its public availability is determined;
(4)(BB) other records as ordered by the court under Rule 4-202.04.

(5) The following court records are protected:[7]
(5)(A) attorney's work product, including the mental impressions or legal theories of an attorney or other representative of the courts concerning litigation, privileged communication between the courts and an attorney representing, retained, or employed by the courts, and records prepared solely in anticipation of litigation and not subject to discovery;
(5)(B) bids or proposals until the deadline for submitting them has closed;
(5)(C) budget analyses, revenue estimates, and fiscal notes of proposed legislation before issuance of the final recommendations in these areas;
(5)(D) budget recommendations, legislative proposals, and policy statements, that if disclosed would reveal the court's contemplated policies or contemplated courses of action;
(5)(E) court security plans;
(5)(F) investigation and analysis of loss covered by the risk management fund;
(5)(G) investigative subpoenas under Utah Code Section 77-22-2;
(5)(H) memorandum prepared by staff for a member of any body charged by law with performing a judicial function and used in the decision-making process;
(5)(I) confidential business records under Utah Code Section 63G-2-309;
(5)(J) a record classified as protected by a governmental entity and shared with the court under Utah Code Section 63G-2-206;
(5)(K) record created or maintained for civil, criminal, or administrative enforcement purposes, audit or discipline purposes, or licensing, certification or registration purposes, if the record reasonably could be expected to:
(5)(K)(i) interfere with an investigation;
(5)(K)(ii) interfere with a fair hearing or trial; or
(5)(K)(iii) disclose the identity of a confidential source;
(5)(L) record identifying property under consideration for sale or acquisition by the court or its appraised or estimated value unless the information has been disclosed to someone not under a duty of confidentiality to the courts;
(5)(M) record that would reveal the contents of settlement negotiations other than the final settlement agreement;
(5)(N) record the disclosure of which would impair governmental procurement or give an unfair advantage to any person;

[7] 4) The following may access a protected court record: (4)(A) the person or governmental entity whose interests are protected by closure; (4)(B) the attorney for the person or governmental entity whose interests are protected by closure or an individual who has a power of attorney from such person or governmental entity; (4)(C) the parent or guardian of the person whose interests are protected by closure if the person is an unemancipated minor or under a legal incapacity; (4)(D) a person with a notarized release from the person or governmental entity whose interests are protected by closure or their legal representative dated no more than 90 days before the date the request is made; (4)(E) a party or attorney for a party to litigation in which the record is filed; (4)(F) the person who submitted the record; (4)(G) anyone by court order; (4)(H) court personnel, but only to achieve the purpose for which the record was submitted; (4)(I) a person provided the record under Rule 4-202.04 or Rule 4-202.05; and (4)(J) a governmental entity with which the record is shared under Rule 4-202.10. Utah Court Rule 4-202.01(4).

(5)(O) record the disclosure of which would interfere with supervision of an offender's incarceration, probation or parole;
(5)(P) record the disclosure of which would jeopardize life, safety or property;
(5)(Q) search warrants and search warrant affidavits before the filing of the return;
(5)(R) strategy about collective bargaining or pending litigation;
(5)(S) test questions and answers;
(5)(T) trade secrets as defined in Utah Code Section 13-24-2;
(5)(U) record of a Children's Justice Center investigative interview before the conclusion of any legal proceedings; and
(5)(V) other records as ordered by the court under Rule 4-202.04

Washington State:
General Rule of Court 31 ACCESS TO COURT RECORDS
(g) Bulk Distribution of Court Records

(1) A dissemination contract and disclaimer approved by the JIS Committee for JIS records or a dissemination contract and disclaimer approved by the court clerk for local records must accompany all bulk distribution of court records.

(2) A request for bulk distribution of court records may be denied if providing the information will create an undue burden on court or court clerk operations because of the amount of equipment, materials, staff time, computer time or other resources required to satisfy the request.

(3) The use of court records, distributed in bulk form, for the purpose of commercial solicitation of individuals named in the court records is prohibited.

North Dakota
N.D. Sup. Ct. Admin. R.
RULE 41. ACCESS TO COURT RECORDS
Section 4. Methods of Access to Court Records.

(c) Requests for Bulk Distribution of Court Records.
(1) Bulk distribution of information in the court record is permitted for court records that are publicly accessible under Section 3(a).
(2) A request for bulk distribution of information not publicly accessible can be made to the court for scholarly, journalistic, political, governmental, research, evaluation or statistical purposes when the identification of specific individuals is ancillary to the purpose of the inquiry. Prior to the release of information under this subsection the requestor must comply with the provisions of Section 6.
(3) A court may allow a party to a bulk distribution agreement access to birth date, street address, and social security number information if the party certifies that it will use the data for legitimate purposes as permitted by law.
(d) Access to Compiled Information From Court Records.
(1) Any member of the public may request compiled information that consists solely of information that is publicly accessible and that is not already in an existing report. The court may compile and provide the information if it

determines, in its discretion, that providing the information meets criteria established by the court, that the resources are available to compile the information and that it is an appropriate use of public resources. The court may delegate to its staff or the clerk of court the authority to make the initial determination to provide compiled information.

(2) Requesting compiled restricted information.

(A) Compiled information that includes information to which public access has been restricted may be requested by any member of the public only for scholarly, journalistic, political, governmental, research, evaluation, or statistical purposes.

(B) The request must:

(i) identify what information is sought,

(ii) describe the purpose for requesting the information and explain how the information will benefit the public interest or public education, and

(iii) explain provisions for the secure protection of any information requested to which public access is restricted or prohibited.

(C) The court may grant the request and compile the information if it determines that doing so meets criteria established by the court and is consistent with the purposes of this rule, the resources are available to compile the information, and that it is an appropriate use of public resources.

(D) If the request is granted, the court may require the requestor to sign a declaration that:

(i) the data will not be sold or otherwise distributed, directly or indirectly, to third parties, except for journalistic purposes;

(ii) the information will not be used directly or indirectly to sell a product or service to an individual or the general public, except for journalistic purposes; and

(iii) there will be no copying or duplication of information or data provided other than for the stated scholarly, journalistic, political, governmental, research, evaluation, or statistical purpose.

The court may make such additional orders as may be needed to protect information to which access has been restricted or prohibited.

Current Access

The Judicial Department collects a significant amount of information from litigants. The reason for collecting this information is for the Department to provide fair, timely and constructive resolution of cases and to enhance public safety. The majority of the information that is collected is required by the court; it is not a voluntarily submitted. The Judicial Department collects and maintains this information for many purposes: processing criminal and traffic cases; collecting fines, fees, surcharges and restitution; registering a protection order; dissolving marriages; providing support for children; obtaining jurors; supervising offenders; settling business disputes; and entering civil judgments. It is for these functions that the Judicial Department's case management system was created.

While it is important for electronic court records to be public for purposes of government accountability and transparency; it is also imperative that the participants' privacy remain intact. If privacy is compromised, the Task Force is concerned that the courts will become less effective. People will lose

their trust in the system because they will be required to divulge private information that may ultimately become public. Using these governing and balancing principles, the Public Access Committee created policies that provide the guidance to offer the access that is currently available to the public and to commercial vendors. The current access provides electronic court records in a real-time environment on a name-by-name or case-by-case basis.

The only direct access that the Judicial Department currently provides is on a case-by-case or name-by-name basis to Government Agency users. This access is provided without charge through a web-based application to government agencies that are required to access court records for their Agency's business operations.

In addition to the direct access provided to Government agency users, an XML access protocol was developed that allows vendors' customers to pass-through their system directly to the Judicial Department's public access database so that the customers can access court records real-time on a name-by-name or case-by-case basis. Any court records that contain identifying information that are available on the vendors website are required to be displayed directly from this database so that the records being accessed are current. At the time of this report, there are two vendors that have elected to access court records using the XML access protocol option; Background Information Services (BIS) and Acxiom.

Data Replication Access

Vendors requested that the Department review its policy regarding data replication. In response to this request, a Task Force was convened to examine the feasibility of such access as well as advantages of determinants and provide recommendations to the Public Access Committee. Data replication access would require the Judicial Department to provide the entire court record database to commercial vendors. The Department would remove protected and non-public information prior to replicating data to the vendors. The vendor would maintain this database on their system/server. The vendor would create a web-based application for their customers to access the data directly from the database they maintain rather than directing the customer to the live Judicial Department's database.

Data Replication Advantages

Vendors have raised some performance and availability concerns with the current real-time data access. There are potential improvements to a vendor's system that could be realized if the vendor maintains the database directly on its servers rather than passing through to the Judicial Department's database. One such improvement would be that the vendor would not have to identify when the system is down (not live). Because the database would be stored on their servers, the vendor would be able to continue to provide access to their customers whether or not the connection to the Judicial Department is live.

Though rare, there have been occasions when connectivity between the two vendors and the Judicial Department was unavailable for short periods of time. When this occurred, the Department returned a message that indicated the system was temporarily unavailable. If vendors maintained the database on their servers, the vendor could continue to allow searches during a potential network outage. However, searches conducted during a period of time in which real-time data replication has been disrupted, the

court records may become stale. The longer that stale data is accessed, the less accurate the court records become. In this situation, it would also be difficult for the Judicial Department to ensure that the vendor returned to a live data display when the connectivity is restored.

Because searches would be handled internally on the vendor's system, it is possible that search functionality and speed could be improved. Localized vendor data stores could provide some efficiency by eliminating search traffic between the Department's network and vendor's network. Discussions with one of the Department's current vendors identified that there could be additional realized performance improvements through the implementation of in-memory data processing.

Data Replication Disadvantages

Once a database is released, the database is completely in control of the recipient. Not only can the recipient manipulate the data in their possession; but the recipient can also copy the database. Since display limitations would be managed locally, the recipient of the data could do anything with the data. There is no way for the Judicial Department to audit the use or location of the data once it is released to the recipient, including copies that the recipient may provide to other entities or subscribers.

Localized data stores created through data replication by itself create inefficiencies and can seriously damage the reputation and lives of others if the recipient fails to receive real-time updates due to technical difficulties or network outages. Ten to fifteen years ago, creating duplicative databases would have been a viable option given the technological limitations of processing real-time data across networks so that recipients would receive the data near instantaneous. Today, those technological limitations no longer exist in that many web service protocols exist to transfer real-time data to requesters of the information within seconds or less. Many of these web service protocols were designed and created to eliminate the inefficiencies of duplicating data stores. Such inefficiencies might include, but not are not limited to, unnecessary storage needs for the recipients of the replicated data, maintaining synchronization of records during network or server outages, maintenance of database table structures, and the amount work it takes to upgrade replication software between two or more entities and its impact on other systems. When data replication fails between one or more entities, the risk of displaying stale or inaccurate information can be damaging to the lives of others. According to a recent Associated Press article titled "AP Impact: When Your Criminal Past Isn't Yours," [8] others can suffer devastating consequences when government agencies erase criminal conviction information yet commercial databases are not updated to reflect this information due to a myriad of technical and negligent factors.

The Judicial Department's database is a very large and complex relational database. The structure is complicated and will become even more complicated and highly normalized –a method by which the database is designed to maintain the integrity of the data while also eliminating redundant data—with the implementation of its new case management system (jPOD). If the entire database is released to vendors, judicial staff will need to train vendors to understand the complexities of Judicial's database so vendors can display the information correctly. The Department at this time is not staffed to conduct such training. The current XML access allows certain fields of data to be mapped to specific data fields in the vendors' systems and not a database.

[8] Robertson, Jordan (2011, December 16). AP Impact: When Your Criminal Past Isn't Yours. Associated Press. Retrieved December 19th, 2011, from http://news.yahoo.com/ap-impact-criminal-past-isnt-yours-182335856.html

Another significant concern raised by database replication is the possibility that recipients may use the data to create statistics that are inaccurate. The very nature of a relational database means that similar data is stored in different tables. When a database is manipulated by persons that are not familiar with the data entry, coding or work processes, untrained individuals extracting composite data may compile inaccurate reports or statistics. Though composite data access requests are submitted to the Judicial Department, judicial staff has the data structure knowledge and technical ability to create accurate reports.

Currently, only certain search capabilities have been approved for the public by the Public Access Committee. The purpose of providing these specific searches is to meet the demand of providing court records for background investigations. The approved search parameters are searches conducted by name or by case number. Searches can be refined with additional filters within these parameters (such as "all" or specific counties, date range of case filings, type of case, date of birth of party, etc.). Vendors are limited to these specific searches by the current XML access. Name searches are complete searches because these searches include accessing all case Registers of Actions that are returned when searching for a specific name.

There are variable costs associated with providing data replication. These include programming, and hardware costs (CPU utilization cost). Programming would be necessary to remove sealed and confidential cases as well as redact confidential information within cases. The Task Force anticipates that additional vendors may be interested in data replication because of the commercial value of data releases. Judicial staff and programmers would also need to assist and train receiving companies to understand the database structure, the relationships between the many tables, and how to correctly display and aggregate the fields. This process can be extremely time intensive and the Department is not staffed to perform such work. Currently Judicial does not have sufficient staff to support multiple vendors maintaining the Judicial Department's replicated database. From a hardware cost perspective, additional CPU (Central Processor Units) on Department servers would be necessary to support increased CPU utilization, which is precipitated by configuring multiple data replication targets.

Database replication would also require the Judicial Department to revisit the pricing structure of providing data to vendors. A per search fee is not suitable because the vendor would have complete control over the database and there is no method for the Judicial Department to identify the number of searches that a vendor conducts against a localized database. A new pricing structure would need to be created that allows the Department to continue to collect sufficient fees to fund the personnel and system hardware necessary to sustain the public access project. These fees are currently collected on a nominal per search fee ($1.75 to $2.25 per search depending on the quantity of searches a vendor conducts).

Regular audits would be imperative. It would be vital to confirm that the vendors are displaying the data correctly, displaying updated (live) information, and timely removing information that has been deleted or sealed by the court. Additionally, vendors would be responsible to obtain licensing to receive replicated data and would have to maintain current licenses. Security protocols would have to be in place to assure the security of the data. At this time Judicial does not have sufficient staff to devote to auditing these concerns.

Technology Options & Barriers

Due to technological advancements in data transfer protocols such as web services and Service Oriented Architectures (SOA), industry standards are moving away from the replication and duplicative databases in favor of web services. Web service protocols and architectures such as Representational State Transfer (REST) were developed to house data in a central location that others can access and keep current and updated. In rare situations where web services may become unavailable due to network or server outages, the entity displaying the information can produce a "temporarily unavailable" notification to requesters of the information rather than supplying stale or static data if the data were localized. Network and server outages are infrequent, and proper disaster recovery measures have been put in place to ensure failover services are provided in the event of a server outage. The Judicial Department is working on redundant network paths in the event a primary network outage occurs.

While data replication technology does exist that allows the transfer of real-time data to various targets or data stores, to configure and maintain replication between one more systems would require significant work. Data replication technologies also make the process of expunging personal identifying information within textual data fields more difficult when data is normally configured to map data field to data field. With a web service approach, the Department can program to remove any personal identifying information prior to transmission.

Vendors have advised the Judicial Department that if data were replicated to outside vendors, they believe they could realize significant search performance improvement through the use of in-memory database processing. This concept is quite intriguing and the Department has researched a variety of solutions to provide an in-memory service to current vendors. Although throughput through the Department's existing web service protocol—previously referred to as XML access—is fast (measured in seconds dependent on the nature of the search parameters), implementation of an in-memory database on behalf of the Judicial Department could significantly improve performance to reduce this time to milliseconds and quite possibly microseconds. However, the Judicial Department has found that implementation of an in-memory database is limited to the number of table joins, thus de-normalized tables would need to be created that are specific to search criteria and results. The Department is very interested in implementing such a solution to its vendors, but would need the time, budget, and resources dedicated to the project.

From an information security perspective, the Judicial Department has a limited ability to ensure personal identifying information is secure at rest and during transmission when data is replicated to outside entities. Once unstructured data leaves the judicial network, the Department forfeits the integrity and security of the information, which ultimately puts the public at risk. While audits are necessary, the Judicial Department is not staffed or funded at this time to conduct such audits.

While there are many flavors of technology to solve various business needs, the Department must ensure that court and probation business needs are carefully blended and aligned with the technology. One cannot drive the other and both must exist to increase efficiencies in providing a fair and impartial system of justice. Therefore, the Judicial Department must carefully examine the business requirements and how those requirements could pose opportunities or threats to internal and external environments before deciding on a technical solution.

Vendor Questions

In an effort to fully understand and identify the desires of the Judicial Department's current public access commercial vendors (BIS and Acxiom), the Task Force identified the following questions for the vendors to answer in order to help guide potential satisfactory solutions:

1. Identify exactly what you would like the Judicial Department to provide.
2. Describe the benefits of receiving replicated data.
3. Describe the detriments of receiving replicated data.
4. What technical solutions would you recommend to transfer/receive replicated data?
5. How would you maintain the integrity, safety and security of the data?
6. If the database were not replicated, what solutions (if any) would you recommend to improve the current search capabilities?
7. Other Comments (feel free to include) issues/factors that you would like the Committee to consider as they review this piece of the Public Access policy.
8. Identify a contact person and the author of the submission for the Committee (or representative) to contact if there are questions or further clarification that is needed.

Vendor Responses

Background Information Services (BIS)

The Judicial Department and Public Access vendors constitute a partnership serving the public; Background Information Services (BIS) is respectfully providing suggestions, which will improve its service to its end users and as a result potentially improve the image of both the Judicial Department and BIS, and increase system usage.

Over the last two decades BIS has obtained Judicial Department data via magnetic tape, Extended Markup language inquiries (XML) from CoCourts, replicated data from Judicial through CoCourts, XML from Lexis-Nexis, and currently XML directly from the Judicial Department. Experience has shown BIS that building its system on a replicated database functions much better than the other modes of operation.

A recurring complaint from BIS customers is that the system, as currently constituted, performs slowly and has too many outages. A glance at the numbers supports this. Of the 915,532 name searches logged year-to-date, only 40,079 had a response time of one second or less. Ten years ago, with far slower computers, but with replicated data, all BIS searches had a response time of less than one second. Widespread Internet usage has raised the bar and one second is now the expected norm. 652,948 searches were logged at two seconds, 181,444 at three seconds, the remaining 22,249 four seconds and over. Four seconds may not appear to be a long time, but it is close to the point at which the user wonders if something has malfunctioned, especially in an era where free services like Google have established excellent service.

18,812 searches returned no result; considering BIS volume of roughly 4000 searches/day, this non-response rate is equivalent to nine half-day outages, and generates dissatisfaction and many telephone calls to BIS.

To address Ms. Linda Bowers list of questions:

1. ***Identify exactly what you would like the Judicial Department to provide.***
   Direct data replication would rectify the above problems. Both BIS and Judicial use Metro Optical Ethernet (MOE); data could be replicated over a fast, secure, and relatively inexpensive path.
2. ***Describe the benefits of receiving replicated data.***
   Replicated data would improve reliability and speed, consequently customer satisfaction. This would also enable BIS the basis to provide Lexis-Nexis with the "Alerts" function in the format they require for it to be useful to them.
3. ***Describe the detriments of receiving replicated data.***
   Data replication would require set-up time by the Judicial Department. When replication was set-up approximately ten years ago, it required Mr. Robert Reynolds about two week's work spread over a calendar month. Costs would need to be analyzed, but are likely to be chiefly on BIS's side.
4. ***What technical solutions would you recommend to transfer/receive replicated data?***
   IBM's replication product, as is now in use by the Judicial Department appears to be the best choice for replication; as mentioned earlier, MOE could provide the replication path.
5. ***How would you maintain the integrity, safety and security of the data?***
   The target computer at BIS would be on an isolated network, accessible only by the Judicial Department and a separate Internet-facing system which would answer external inquiries. BIS

utilizes both a Cisco Firewall, and Cisco Intrusion Detection System, specifically a 6500 FWSM and an IDS-2.

6. ***If the database were not replicated, what solutions (if any) would you recommend to improve the current search capabilities?***
   Without a careful analysis of the Judicial Department's internal systems, it is difficult for BIS to make recommendations for alternatives within the Department.
7. ***Other Comments (feel free to include) issues/factors that you would like the Committee to consider as they review this piece of the Public Access policy.***
   BIS has been pleased to be one of the Judicial Department's partners in the public access effort and has developed a good working relationship and respect for the Department's technical staff. BIS currently pays the Judicial Department $1.7 million per year for data access, consequently has assisted the Department in a significant, material manner.
8. ***Identify a contact person and the author of the submission for the Committee (or committee representative) to contact if there are questions or further clarification that is needed.***
   Please contact John Nebel, john.nebel@csd.net 303-618-7345 with questions.

Acxiom

No written response at this time.

Conclusion and Task Force Recommendations

Chief Justice Directive 05-01's purpose is to provide reasonable access to court records while simultaneously ensuring confidentiality in accordance within existing laws, policies and procedures. To do this, access must be in a manner that: maximizes accessibility to court records; supports the role of the judiciary; promotes governmental accountability; contributes to public safety; minimizes risk of injury to individuals; protects individual privacy rights and interests; protects proprietary business information; minimizes reluctance to use the court to resolve disputes; makes effective use of court and clerk of court staff; provides excellent customer service; does not unduly burden the ongoing business of the judiciary; and protects individuals from the use of outdated or inaccurate information. [9]

When conducing the necessary research to compile the data replication report, the Task Force acknowledged the need to balance a variety of competing public access principles, that are aligned with CJD 05-01 including the public's expectation to access court records in a variety of mediums, a duty to protect sealed and confidential information in court and probation records, and a duty to respond to record requests in a timely and efficient manner from public and private entities. The difficulty with addressing policy modifications is to remember that the access to the public must be the same for everyone: vendors, media, commercial entities, and all other persons requesting the information. While the Department currently contracts with only two vendors, the Task Force anticipates that other vendors and commercial entities will desire data replication access because of the commercial value of the complete database. Currently, these other vendors and commercial entities still access the court records, but they must obtain the information using one of the current vendors systems rather than using a direct XML pass-through to the Department's system.

[9] http://www.courts.state.co.us/Courts/Supreme_Court/Directives/05-01%20policyAMENDED07-26-11.pdf

After weighing the factors, the Task Force makes the following observations and recommendations.

1. Current access to electronic court data is appropriate and sufficient. The process of allowing vendors to access electronic court records using Web Service or XML pass-through protocol provides complete, accurate and up-to-date records. If data replication becomes an option for electronic record release, it is probable that additional vendors would obtain this type of access, which opens the door to a variety of problems such as those outlined in the Data Replication Disadvantages section.

2. Data and information from a replicated database cannot be sufficiently protected. It would be impossible for the Department to identify where the database may be sold once it leaves the Department as a replicated database. This means that case information that could be available on the Internet may be stale and therefore inaccurate. It would also be impossible to ensure that previously released records are sealed when the court so orders.

3. If access to court and probation records were to change to a replication model, the accuracy of data displays could not be sufficiently monitored. The Department's electronic databases are extremely large and complex. Department resources would be required to providing training regarding table joins and data display to customers receiving the replicated data. Because of the database complexities, if the data were to be released without training for the companies receiving the data, records may be displayed and publicly available with inaccurate information associated with individuals. Furthermore, the Department would have no mechanism to ensure the release of any replicated data is accurate and complete at all times, and that the data is not being sold or redistributed to other entities. At this time, the Department does not have sufficient extra resources to make changes to data access and must use its resources to focus on other projects that are currently in development.

4. Discussion with other members of the Government Data Advisory Board (GDAB) and CICJIS, the Task Force identified that it is extremely uncommon for other Colorado governmental agencies to replicate data to a central data warehouse, let alone to replicate data repositories among multiple agencies. The architecture of such high-volume and large-scale data transformation systems is to use query pass through technologies such as Service Oriented Architecture (SOA). Given that many other agencies across the state see the inefficiencies found in storing duplicative data, it is the Task Force recommendation not create such inefficiencies with other private entities when the Department has established the proper Web Service architecture to retrieve data.

Therefore, the Task force believes that appropriate {and sufficient} access to electronic court data currently exists. In light of the purpose of CJD 05-01 (Section 1.00(a)), the concerns discussed in this report regarding stale and inaccurate information and parties' privacy outweighs changing the policy related to data replication at this time.

Though it is premature to change the access policy at this time, the Task Force recommends that the Department continue to research technology opportunities that may enhance performance of the current system. Additionally, it is the Task Force's recommendation that the Department continue to review additional access options as technology changes/improves.

ATTACHMENT A

The New York Times

December 16, 2011

AP IMPACT: When Your Criminal Past Isn't Yours

By THE ASSOCIATED PRESS

SAN FRANCISCO (AP) — A clerical error landed Kathleen Casey on the streets.

Out of work two years, her unemployment benefits exhausted, in danger of losing her apartment, Casey applied for a job in the pharmacy of a Boston drugstore. She was offered $11 an hour. All she had to do was pass a background check.

It turned up a 14-count criminal indictment. Kathleen Casey had been charged with larceny in a scam against an elderly man and woman that involved forged checks and fake credit cards.

There was one technicality: The company that ran the background check, First Advantage, had the wrong woman. The rap sheet belonged to Kathleen A. Casey, who lived in another town nearby and was 18 years younger.

Kathleen Ann Casey, would-be pharmacy technician, was clean.

"It knocked my legs out from under me," she says.

The business of background checks is booming. Employers spend at least $2 billion a year to look into the pasts of their prospective employees. They want to make sure they're not hiring a thief, or worse.

But it is a system weakened by the conversion to digital files and compromised by the welter of private companies that profit by amassing public records and selling them to employers. These flaws have devastating consequences.

It is a system in which the most sensitive information from people's pasts is bought and sold as a commodity.

A system in which computers scrape the public files of court systems around the country to retrieve personal data. But a system in which what they retrieve isn't checked for errors that would be obvious to human eyes.

A system that can damage reputations and, in a time of precious few job opportunities, rob honest workers of a chance at a new start. And a system that can leave the Kathleen Caseys of the world — the innocent ones — living in a car.

Those are the results of an investigation by The Associated Press that included a review of thousands of pages of court filings and interviews with dozens of court officials, data providers, lawyers, victims and regulators.

"It's an entirely new frontier," says Leonard Bennett, a Virginia lawyer who has represented hundreds of plaintiffs alleging they were the victims of inaccurate background checks. "They're making it up as they go along."

Two decades ago, if a county wanted to update someone's criminal record, a clerk had to put a piece of paper in a file. And if you wanted to read about someone's criminal past, you had to walk into a courthouse and thumb through it. Today, half the courts in the United States put criminal records on their public websites.

Digitization was supposed to make criminal records easier to access and easier to update. To protect privacy, laws were passed requiring courts to redact some information, such as birth dates and Social Security numbers, before they put records online. But digitization perpetuates errors.

"There's very little human judgment," says Sharon Dietrich, an attorney with Community Legal Services in Philadelphia, a law firm focused on poorer clients. Dietrich represents victims of inaccurate background checks. "They don't seem to have much incentive to get it right."

Dietrich says her firm fields about twice as many complaints about inaccurate background checks as it did five years ago.

The mix-ups can start with a mistake entered into the logs of a law enforcement agency or a court file. The biggest culprits, though, are companies that compile databases using public information.

In some instances, their automated formulas misinterpret the information provided them. Other times, as Casey discovered, records wind up assigned to the wrong people with a common name.

Another common problem: When a government agency erases a criminal conviction after a designated period of good behavior, many of the commercial databases don't perform the updates required to purge offenses that have been wiped out from public record.

It hasn't helped that dozens of databases are now run by mom-and-pop businesses with limited resources to monitor the accuracy of the records.

The industry of providing background checks has been growing to meet the rising demand for the service. In the 1990s, about half of employers said they checked backgrounds. In the decade since Sept. 11, that figure has grown to more than 90 percent, according to the Society for Human Resource Management.

To take advantage of the growing number of businesses willing to pay for background checks, hundreds of companies have dispatched computer programs to scour the Internet for free court data.

But those data do not always tell the full story.

Gina Marie Haynes had just moved from Philadelphia to Texas with her boyfriend in August 2010 and lined up a job managing apartments. A background check found fraud charges, and Haynes lost the offer.

A year earlier, she had bought a used Saab, and the day she drove it off the lot, smoke started pouring from the hood. The dealer charged $291.48 for repairs. When Haynes refused to pay, the dealer filed fraud charges.

Haynes relented and paid after six months. Anyone looking at Haynes' physical file at the courthouse in Montgomery County, Pa., would have seen that the fraud charge had been removed. But it was still listed in the limited information on the court's website.

The website has since been updated, but Haynes, 40, has no idea how many companies downloaded the outdated data. She has spent hours calling background check companies to see whether she is in their databases. Getting the information removed and corrected from so many different databases can be a daunting mission. Even if it's right in one place, it can be wrong in another database unknown to an individual until a prospective employer requests information from it. By then, the damage is done.

"I want my life back," Haynes says.

Haynes has since found work as a customer service manager, but she says that is only because her latest employer didn't run a background check.

Hard data on errors in background checks are not public. Most leading background check companies contacted by the AP would not disclose how many of their records need to be corrected each year.

A recent class-action settlement with one major database company, HireRight Solutions Inc., provides a glimpse at the magnitude of the problems.

The settlement, which received tentative approval from a federal judge in Virginia last month, requires HireRight to pay $28.4 million to settle allegations that it didn't properly notify people about background checks and didn't properly respond to complaints about inaccurate files. After covering attorney fees of up to $9.4 million, the fund will be dispersed among nearly 700,000 people for alleged violations that occurred from 2004 to 2010. Individual payments will range from $15 to $20,000.

In an effort to prevent bad information from being spread, some courts are trying to block the computer programs that background check companies deploy to scrape data off court websites. The programs not only can misrepresent the official court record but can also hog network resources, bringing websites to a halt.

Virginia, Arizona and New Mexico have installed security software to block automated programs from getting to their courts' sites. New Mexico's site was once slowed so much by automated data-mining programs that it took minutes for anyone else to complete a basic search. Since New Mexico blocked the data miners, it now takes seconds.

In the digital age, some states have seen an opportunity to cash in by selling their data to companies. Arizona charges $3,000 per year for a bundle of discs containing all its criminal files. The data includes personal identifiers that aren't on the website, including driver's license numbers and partial Social Security numbers.

Other states, exasperated by mounting errors in the data, have stopped offering wholesale subscriptions to their records.

North Carolina, a pioneer in marketing electronic criminal records, made $4 million selling the data last year. But officials discovered that some background check companies were refusing to fix errors pointed out by the state or to update stale information.

State officials say some companies paid $5,105 for the database but refused to pay a mandatory $370 monthly fee for daily updates to the files — or they would pay the fee but fail to run the update. The updates provided critical fixes, such as correcting misspelled names or deleting expunged cases.

North Carolina, which has been among the most aggressive in ferreting out errors in its customers' files, stopped selling its criminal records in bulk. It has moved to a system of selling records one at a time. By switching to a more methodical approach, North Carolina hopes to eliminate the sloppy record-keeping practices that has emerged as more companies have been allowed to vacuum up massive amounts of data in a single sweep.

Virginia ended its subscription program. To get full court files now, you have to go to the courthouse in person. You can get abstracts online, but they lack Social Security numbers and birth dates, and are basically useless for a serious search.

North Carolina told the AP that taxpayers have been "absorbing the expense and ill will generated by the members of the commercial data industry who continue to provide bad information while falsely attributing it to our courts' records."

North Carolina identified some companies misusing the records, but other culprits have gone undetected because the data was resold multiple times.

Some of the biggest data providers were accused of perpetuating errors. North Carolina revoked the licenses of CoreLogic SafeRent, Thomson West, CourtTrax and five others for repeatedly disseminating bad information or failing to download updates.

Thomson West says it was punished for two instances of failing to delete outdated criminal records in a timely manner. Such instances are "extremely rare" and led to improvements in Thomson West's computer systems, the company said.

CoreLogic says its accuracy standards meet the law, and it seemed to blame North Carolina, saying that the state's actions "directly contributed to the conditions which resulted in the alleged contract violations," but it would not elaborate. CourtTrax did not respond to requests for comment.

Other background check companies say the errors aren't always their fault.

LexisNexis, a major provider of background checks and criminal data, said in a statement that any errors in its records "stem from inaccuracies in original source material — typically public records such as courthouse documents."

But other problems have arisen with the shift to digital criminal records. Even technical glitches can cause mistakes.

Companies that run background checks sometimes blame weather. Ann Lane says her investigations firm, Carolina Investigative Research, in North Carolina, has endured hurricanes and ice storms that knocked out power to her computers and took them out of sync with court computers.

While computers are offline, critical updates to files can be missed. That can cause one person's records to fall into another person's file, Lane says. She says glitches show up in her database at least once a year.

Lane says she double-checks the physical court filings, a step she says many other companies do not take. She calls her competitors' actions shortsighted.

"A lot of these database companies think it's 'ka-ching ka-ching ka-ching,'" she says.

Data providers defend their accuracy. LexisNexis does more than 12 million background checks a year. It is one of the world's biggest data providers, with more than 22 billion public records on its own computers.

It says fewer than 1 percent of its background checks are disputed. That still amounts to 120,000 people — more than the population of Topeka, Kan.

But there are problems with those assertions. People rarely know when they are victims of data errors. Employers are required by law to tell job applicants when they've been rejected because of negative information in a background check. But many do not.

Even the vaunted FBI criminal records database has problems. The FBI database has information on sentencings and other case results for only half its arrest records. Many people in the database have been cleared of charges. The Justice Department says the records are incomplete because states are inconsistent in reporting the conclusions of their cases. The FBI restricts access to its records, locking out the commercial database providers that regularly buy information from state and county government agencies.

Data providers are regulated by the Federal Trade Commission and required by federal law to have "reasonable procedures" to keep accurate records. Few cases are filed against them, though, mostly because building a case is difficult.

A series of breaches in the mid-2000s put the spotlight on data providers' accuracy and security. The fallout was supposed to put the industry on a path to reform, and many companies tightened security. But the latest problems show that some accuracy practices are broken.

The industry says it polices itself and believes the approach is working. Mike Cool, a vice president with Acxiom Corp., a data wholesaler, praised an accreditation system developed by an industry group, the National Association of Professional Background Screeners. Fear of litigation keeps the number of errors in check, he says.

"The system works well if everyone stays compliant," Cool says.

But when the system breaks down, it does so spectacularly.

Dennis Teague was disappointed when he was rejected for a job at the Wisconsin state fair. He was horrified to learn why: A background check showed a 13-page rap sheet loaded with gun and drug crimes and lengthy prison lockups. But it wasn't his record. A cousin had apparently given Teague's name as his own during an arrest.

What galled Teague was that the police knew the cousin's true identity. It was even written on the background check. Yet below Teague's name, there was an unmistakable message, in bold letters: "Convicted Felon."

Teague sued Wisconsin's Department of Justice, which furnished the data and prepared the report. He blamed a faulty algorithm that the state uses to match people to crimes in its electronic database of criminal records. The state says it was appropriate to include the cousin's record, because that kind of information is useful to employers the same way it is useful to law enforcement.

Teague argued that the computers should have been programmed to keep the records separate.

"I feel powerless," he says. "I feel like I have the worst luck ever. It's basically like I'm being punished for living right."

One of Teague's lawyers, Jeff Myer of Legal Action of Wisconsin, an advocacy law firm for poorer clients, says the state is protecting the sale of its lucrative databases.

"It's a big moneymaker, and that's what it's all about," Myer says. "The convenience of online information is so seductive that the record-keepers have stopped thinking about its inaccuracy. As valuable as I find public information that's available over the Internet, I don't think people have a full appreciation of the dark side."

In court papers, Wisconsin defended its inclusion of Teague's name in its database because his cousin has used it as an alias.

"We've already refuted Mr. Teague's claims in our court documents," said Dana Brueck, a spokeswoman for Wisconsin's Department of Justice. "We're not going to quibble with him in the press."

A Wisconsin state judge plans to issue his decision in Teague's case by March 11.

The number of people pulling physical court files for background checks is shrinking as more courts put information online. With fewer people to control quality, accuracy suffers.

Some states are pushing ahead with electronic records programs anyway. Arizona says it hasn't had problems with companies failing to implement updates.

Others are more cautious. New Mexico had considered selling its data in bulk but decided against it because officials felt they didn't have an effective way to enforce updates.

Meanwhile, the victims of data inaccuracies try to build careers with flawed reputations.

Kathleen Casey scraped by on temporary work until she settled her lawsuit against First Advantage, the background check company. It corrected her record. But the bad data has come up in background checks conducted by other companies.

She has found work, but she says the experience has left her scarred.

"It's like Jurassic Park. They come at you from all angles, and God knows what's going to jump out of a tree at you or attack you from the front or from the side," she says. "This could rear its ugly head again — and what am I going to do then?"

___ AP Technology Writer Michael Liedtke in San Francisco contributed to this report.