Title
Practical Obscurity in the Digital Age: Public Records in the Private Sector

Author
Testa-Avila, Evynn

Publication Date
2008-04-01

Practical Obscurity in the Digital Age:
Public Records in the Private Sector

By
Evynn Testa-Avila (evynn.testaavila@gmail.com)
School of Information, UC Berkeley

UCB iSchool Report 2008-022
April 2008

Abstract:
In this paper, I outline the legislative framework governing information privacy practices in the public and private sectors in the United States and, more narrowly, the state of California, with particular attention paid to criminal justice system information. I will explore the relationship between the courts, which maintain public criminal records, and Corporate Data Brokers (CDBs), which aggregate and sell information from court records, as well as the accuracy and privacy of their systems. While legislation guiding the government's handling of information may need to be extended to the private sector, state governments have a role to play in improving their technology infrastructure to ensure that accurate, timely information is available in the public records. This is particularly important for the criminal justice system, the source of data brokers collecting. In making this argument, I look at one state, Colorado, that did a great deal early on to improve their criminal records technology infrastructure.

1.0 Introduction[1]

When public records were kept in paper archives, scattered across numerous agency offices in thousands of localities across the country, the privacy of these records would have seemed to be a minute concern. In order to find information about a person's criminal record, for example, someone would need to visit courthouses in all the municipalities and counties in which the person had lived, and first they would have needed to figure out where the person had lived. Things have changed, and in ways that are not as obvious as they might appear at first glance. Of course, technology has made information pervasive and often easily accessed on the Web. But certain kinds of data, about a person's arrest or conviction records, are still not widely accessible to anyone with idle curiosity and a browser. With the exception of a few regions of the country, these records are often only available to those members of the general public who are willing to go to the county courthouse and dig through paper files.

The important change is not in government information practices, which, while they sometimes lag in technology adoption, have become stricter and more accountable in the past few decades, but in the private sector. Corporate data brokers (CDBs), such as ChoicePoint, collect information on individuals from all over the country, amassing huge databases of personal information that they then sell to government agencies, insurers and private sector employers, among others. These services are immensely valuable—ChoicePoint is being acquired by Reed Elsevier for 4.1 billion dollars[2]—and the data in

[1] The following individuals have contributed enormously to this paper through conversations, reading of drafts and insightful critiques: Chris Volz, Bob Glushko, Eric Kansa, Jeff Selbin, Chris Hoofnagle and Eliza Hersh.

[2] http://www.reed-elsevier.com/index.cfm?articleid=2200

these databases can determine whether a person gets a job, a professional license or insurance, so errors have serious consequences. Yet few people are aware of the existence of CDBs until something goes wrong, and there is very little legislation governing how they collect and use information.

In this paper, I outline the legislative framework governing information privacy practices in the United States and, more narrowly, the state of California and the issues of information accuracy and privacy that CDBs need to be concerned with. I will argue that the legislation guiding the government's handling of information needs to be extended to the private sector, but that state governments have a role to play in improving their technology infrastructure to ensure that accurate, timely information is available in the public records, particularly in the criminal justice system, that data brokers collect from. In making this argument, I look at one state, Colorado, that did a great deal early on to improve their criminal records technology infrastructure. These improvements to infrastructure and updated policy would ensure that as information disseminates through public and private sector channels, it remains accurate and timely and that the parties handling it remain accountable. This in turn will improve the quality of services offered by both CDBs and courts.

2.0 Stakeholders: Relationships & Quality

The landscape of stakeholders and services that coalesce to produce CDB background checks is incredibly complex. I will focus on what I see as the four primary stakeholders in the process of criminal records background checks, alluded to in the introduction: CDBs; criminal justice system agencies, especially courts; job and professional license applicants; and employers and licensing agencies. Each of these

stakeholders has unique concerns regarding the accuracy and timeliness of criminal records and their relationship to the other stakeholders. They are also likely to hold different measures of data quality.

2.1 CDBs

CDBs must consider the concerns of both employers and job applicants, the two stakeholders they may provide direct services to. However, influence of the two parties is not equal: CDBs target employers as the customers for their background check products, and employers choose to engage in a customer-service provider relationship with the CDB. They pay for a service and thus help determine its value. The value of that service is greater when they receive information that leads them to hire employees who will not increase their liability as a company and who appear to be trustworthy based on the alignment of their application with the background check.

The best way for the CDB to deliver this value to the employer is to make every effort to ensure the accuracy of their records with respect to convictions. This is not an easy task, considering that CDBs collect data from public records all over the country, from agencies with different information systems, policies and procedures for accessing those records. CDBs must try to make sense of this data and connect the right facts with the right individuals. This takes place internally and the complexity of the process may not be seen or realized by customers who simply receive a report that connects facts and incidents to a name. This part of the service is crucial, but it occurs on the "back stage," that is, it is not exposed to the customer. The "front stage"—the part of the service that is visible to the customer, is a completed background report. (Teboul, 2006; Glushko & Tabas 2007)

2.2 Employers: Avoiding Liability

More and more employers have begun performing background checks; in fact, one survey found that 96% of employers ran checks on applicants in 2004. (Greenwald, 2007) Background checks offer employers a presumably objective and accurate means of confirming the honesty of an applicant's answers to questions in the application and interview. Furthermore, employers may be held liable if they hire an employee whose criminal background poses a risk to their business (say, a drug offender trying to work as a hospital orderly with access to prescription medication).

While employers doubtless wish to have the most accurate information possible when making hiring decisions, however, this concern may be biased. Specifically, employers may be inclined to prefer inaccurate negative information over falsely positive information, since overall this will decrease the employer's liability inappropriate hiring decisions. This preference is almost certainly counteracted by the employer's desire not to pass up qualified applicants due to inaccurate reports on convictions, but accuracy may not be the primary concern here.

2.3 Job Applicants: No-Win Front-stage Service

For job applicants, the quality of the service provided by the CDB is greatest when the CDB is a completely invisible "backstage" player. The applicant may know that a background check is being performed, and knows that this check will be a factor in the decision to hire them. But, unless negative information turns up they may never know which company provided it and they almost certainly would not see a reason to contact that CDB. The interaction the job applicant has with the CDB will, at best, allow him to learn the source of the adverse information on the background check and perhaps see a

copy of the check. A CDB cannot change erroneous information regarding criminal convictions or remedies unless these changes are derived from the public record. The service they provide to applicants is limited and will not fulfill the job applicant's ultimate goal of removing or changing the conviction data that appears on their background check. Thus, the service encounter between the job applicant and the CDB is inherently negative.

2.4 Courts: Everything to Everyone

The courts, where criminal conviction records originate, have what is probably the most ambiguous and complex role in the matter. Part of the difficulty lies in the policy and legal surrounding access public records discussed in Section 3, but the role of the courts as service providers, and indeed the question of whether they ought even to prioritize customer service, is fraught.[3] Courts, unlike private companies and like other public sector agencies, cannot target those segments of the market that are easiest or most profitable to serve nor can they deny service based on dissatisfaction with the behavior of a particular customer or group. (Fountain, 2001) In the interest of equality, courts must respond to every petition for dismissal as well as requests for public records from members of the public, which may include CDB employees.

The former group— the petitioners— often approach the court without much knowledge of how the process works or what remedy they should seek. This can put court clerks in the awkward position of advising petitioners of which remedies to seek,

[3] See Fountain, Jane, *Paradoxes of Public Sector Customer Service* for an extensive discussion of the potential difficulties encountered in trying to align public sector agencies with private sector customer service practices.

which can result in remedies being granted that the petitioner does not qualify for.[4] It is unclear what the consequences of such mistakes would be if they make it all the way to a background check, but it certainly lowers the quality of the data and thus the quality of the service provided to CDBs and, indirectly, to employers.

The CDB, in turn, has service needs that many courts may not be able to meet due to lack of resources. For many areas of the country, the only way to get court records is to go to the courthouse, look up a case docket number then find the associated paper documents in an archive. Other courts[5] provide electronic versions of conviction records. While this is a potential source of revenue for the court and can provide CDBs with a valuable service, there is concern in the legal community over the policy regarding the use of such records. Currently, Ohio is considering a rule change[6] to allow such sales of records, but legal aid organizations are concerned that the rule does not have stringent enough requirements to ensure that customers buy records frequently and thus stay up-to-date.

Thus, the courts face a multitude of demands from different parties that they ill-equipped to handle in a timely, accurate manner and that bring up serious policy questions. Their "customer" is only nebulously defined (Fountain, 2001), and includes segments of the public whose interests are directly opposed to one another. The court system must provide all these services to the public, but since the demand is high and

[4] One such instance appears on a RAP sheet (with personal information redacted) used as an example by the East Bay Community Law Center, the client organization backing this project. It shows that one conviction was dismissed under California Penal Code 1203.4, and also that the person served time in state prison for the same conviction, whereas one of the requirements for this type of dismissal is that the person not have spent time in prison for the conviction.

[5] Denton County, TX: http://justice.dentoncounty.com/records.htm; Charlotte County FL: http://www.co.charlotte.fl.us/OLD_WEB_PAGES/public/OR_access_levels.htm;

[6] PC, Jeff Selbin 12/18/2007 Email "[Fwd: Ohio rule change re: selling criminal record/court data]"

resources low, the quality of the service is likely to be vary greatly depending on how much each court considers the service to be a core part of its mission.

3.0 Uneasy Balance: Data Privacy & Accuracy

Any agency, in the public or private sector, that collects and maintains information about individuals must be concerned with two issues: protecting the privacy of those individuals while satisfying the need for information to be accessible and ensuring the accuracy of the information about them. These goals are not always in harmony. Ensuring absolute accuracy may mean undue prying into an individual's personal life, compromising privacy. Fortunately, though, the interests of government, individuals, data brokers and employers do overlap in crucial ways.

3.1 Data Accuracy

CDBs, employers who buy their services, the government and individuals all have some interest in ensuring that data about individuals' criminal records is accurate and timely. Individuals, obviously, do not want inaccurate information regarding their criminal past to jeopardize their chances at gaining employment. Individuals should not need to worry about convictions that have been dismissed appearing as non-remedied convictions in their background checks for private employers, nor should they be vulnerable to blatantly false information about non-existent convictions. Employers need accurate information to ensure they do not expose themselves to liability for hiring employees with certain types of convictions, but also to ensure that qualified applicants are not passed over because of inaccurate information about a criminal past.

Several cases have been filed in state and regional courts alleging that ChoicePoint provided inaccurate information to prospective employers and insurers. In Johnson v. Choicepoint,[7] filed in the US District Court for the Eastern District of Louisiana, ChoicePoint was accused of having inaccurately reported to an employer that the plaintiff had a criminal conviction; the mistake was corrected and a settlement reached. Privacy advocates who have requested or obtained reports from the company have found them riddled with errors, including unwarranted suggestions that they may have criminal records, had been married to unknown persons or were dead. (Sullivan, 2005) ChoicePoint infamously provided the state of Florida with the lists of felons to be purged from the voting rolls in 2000, which was later found to be full of errors. (Simpson, 2001)

Unfortunately, it is difficult to determine the accuracy of the information held by CDBs, as they are not generally forthcoming about the details of their information collection and management processes. There is a good deal of anecdotal evidence, and though data brokers would probably claim that these incidents do not reflect the general accuracy of their records, they are the only independent evidence we have to go on.

3.2 Data Privacy

The past forty years have seen information technology develop enormously, leading some to fear we are becoming a "Dossier society," (Laudon, 1986) in which the government, or, perhaps more relevant to the current discussion, some shadowy corporation, will gather comprehensive records for every citizen. Some scholars have

[7] *Dorothy Moten Johnson v. Choicepoint Services, Inc., et al*, 2004 U.S. Dist. LEXIS 2009

suggested a need to reconceptualize privacy in light of the pervasiveness of information technology and connectivity. Daniel Solove (2002) has argued that simply because certain information is not secret does not mean it cannot be considered private. Instead, he sees privacy as embodying limits on the accessibility of information. The Supreme Court has also acknowledged a privacy interest when it comes to public records which is protected by the "practical obscurity" of such records—that is, in the world of paper files, it takes some considerable effort to find comprehensive records on an individual. [8]

Solove's work provides a useful framework for discussing the differing perspectives that the stakeholders in question here might espouse. There are a number of laws, both nationally and in the state of California, that govern access to personal information of certain types and in certain contexts: the Fair Credit Reporting Act for financial information, the Health Insurance Portability and Accountability Act for health information and the Investigative Consumer Reporting Agencies Act in California, governing CDBs. These laws balance the need for personal information to flow freely in order to allow people to make crucial decisions with the need for individuals to protect themselves from unwanted and harmful disclosures of their information. CDBs, which collect information that is potentially very damaging and embarrassing to individuals, should be subject to regulations pertaining to how they handle that information as well.

4.0 Existing Information Legislation

In the following section, I look at legislation regarding privacy and handling of information in government agencies. These are the most broadly applicable laws when it

[8] *U.S. Dept. Of Justice V. Reporters Committee,* 489 U.S. 749 (1989)

comes to the type of information covered and their possible uses, and thus they offer a framework for thinking about this type legislation. I also look at one industry-specific law in California: the Investigative Consumer Reporting Agencies Act, which applies explicitly to the practices of CDBs.

4.1 Federal: The Privacy Act

In the 1970s, following a report by the Department of Health, Education and Welfare that articulated a set of "Fair Information Practices," the federal government and many of the states began to enact privacy laws governing the collection, maintenance and use of personal information. The United States Congress passed the Privacy Act in 1974, and many states followed suit with similar laws. The act required that an agency of the federal government must only collect personal information for a specific, legitimate government function; it must allow access and correction mechanisms for data subjects; and it must limit collection to that information that is necessary for fulfilling that specific function. (Hoofnagle, 2004)

The Act applies to information originating with the government and used by government contractors, but does not apply to CDBs that gather the information independently. (Hoofnagle, pc, 2007) This has left the door open for CDBs to gather information from public records and sell comprehensive records on individuals to other companies and even, ironically, to the government.

4.2 California

4.2.1 Information Practices Act

The state of California has a more restrictive set of laws governing information privacy, including legislation that applies specifically to investigative consumer reporting agencies. Besides acknowledging a right to personal privacy explicitly in the state constitution, California passed the Information Practices Act in 1977, drawing on the same principles as the federal government did in constructing the Privacy Act, but expanding them as well. In addition to the requirements of the national Privacy Act, the California law requires agencies to keep a record of the source of information about an individual and, upon transferring any information to another agency, "to correct, update, withhold or delete any portion of a record that it knows or has reason to believe is inaccurate or untimely."

4.2.2 Investigative Consumer Reporting Agencies Act

The Investigative Consumer Reporting Agencies Act (ICRAA) of California governs how companies that collect, maintain and sell information about consumers to employers, insurers, licensing agencies and others. The law defines what parties may request information, under what circumstances and what types of information they may request. Requestors must certify to the consumer reporting agency that they are using the information for a particular, legally sanctioned purpose. It gives consumers the right to view their files, in some cases without charge, and dispute information contained therein. The ICRAA outlines a detailed procedure disputing information in the reporting agencies' file, and requires the agency to investigate on behalf of the consumer and make corrections or, if they cannot confirm the accuracy or correct of the information, delete it.

The ICRAA also sets out very specific guidelines for dealing with public records and especially adverse information, such as convictions, arrests and tax liens, that is

obtained from public records. All information that originates in public records must be accompanied by the source and date of the information. When such information is provided in a report, there are regulations requiring that the information must have been verified within thirty days before issuing the report. Additionally, reports must not contain "…Records of arrest, indictment, information, misdemeanor complaint, or conviction of a crime that, from the date of disposition, release, or parole, antedate the report by more than seven years." (CA Civil Code 1786.18(a) (7))

5.0 Legislating CDBs

California's ICRAA is an excellent example of how states and the national government can go about regulating corporate data brokers. It contains provisions relating to most of the key requirements when it comes to handling information[9]-- regarding information gathering, storage, sale and disposal-- that such legislation should address. Table 1, below, summarizes these requirements and some key questions to address with respect to each:

	Requirement	***Questions to address***
(a)	Verification and accuracy	What measures are CDBs required to take to ensure the accuracy of their records? How long can information of various types be stored and reported?
(b)	Provenance	What information is the CDB required to store regarding the source and initial acquisition date of information?
(c)	Access	What types of agencies have access to information, and in what circumstances? What rights do consumers have to view information about themselves?
(d)	Corrections	How can consumers dispute information in their file? What obligations does the CDB have to investigate and correct disputed information?
(e)	Auditing external use	What is the obligation of the CDB with respect to ensuring

[9] N.B.: The ICRAA also lays out remedies for non-compliance, and these are indeed crucial in any such legislation, however I am concerned here with how data is actually handled.

		lawful and non-abusive use of the information it provides to customers? How must the CDB secure its data against unsanctioned uses?
(f)	Authoritative source	For information available in public records, what is the authoritative source for this information?

Table 1

The first two requirements deal with how CDBs manage the information they have, from acquisition, to reporting (for example, ICRAA provisions that require verification before reporting sensitive information), to disposal. The second two requirements address the relationship between CDBs and the subjects (citizens, consumers, job applicants and others). The fourth requirement deals with how CDBs interact with their customers and suggests that some level of auditing to ensure lawful use is necessary. Finally, the last requirement suggests the need to ensure that data that can be drawn from public records is obtained from the most reliable sources. Most of these issues are addressed in most industry-specific information practices laws, and the California law addresses each of them in detail save the last, authoritative sourcing.[10]

5.1 Authoritative Source

It is important to ensure that personal information, especially about potentially adverse events like a conviction, is obtained from the source that has the most timely version of that information and preferably, where it originated in the official record. This information may not change frequently, but when it does it is crucial that the change is registered at all levels as quickly as possible.

The reason for this recommendation is evident in a case brought against ChoicePoint and Revco Discount Drug Centers/CVS in the US District Court for the

[10] Thanks to Chris Volz for suggesting authoritative sourcing as a consideration.

Western District of North Carolina, Ashville Division.[11] A former employee, Katrina Joiner, of the drug store CVS was terminated after she was caught on tape picking up prescription drugs for her father without the cashier charging her for the co-payment. She signed a statement for her employer admitting that she left the store without paying for the drugs, and was subsequently fired. Joiner contended that the incident was an oversight on the part of herself and the cashier, rather than theft. The employer, however, reported the termination to ChoicePoint giving the reason as a "theft of drugs." This language, by implying a crime and possibly a conviction, led to Joiner losing other job opportunities.

Clearly, ChoicePoint was here only passing along bad information it received from Revco Discount Drug Centers, and in fact ChoicePoint removed the offending phrase from Joiner's record and was dropped from the suit, but this points to a need to ensure information is being properly sourced and verified by CDBs. Job applicants should not have to worry about incidents in which no charges were brought and in which they were not convicted appearing on background checks as apparent convictions. The fact that an applicant has no reason to believe such information would appear in a background check means that they will have no reason to believe they should address it in a job interview, which may make them appear dishonest on top of being a criminal.

This is where the issue of state public records, and specifically criminal records technology infrastructure comes in. States should evaluate, or require that counties within them evaluate, their public records systems to ensure that the information contained is accurate and timely, and has in place appropriate access and usage controls. States should

[11] *Katrina Joiner v. Choicepoint Services, Inc., and Revco Discount Drug Centers, Inc., d/b/a CVS,* 2006 U.S. Dist. LEXIS 70239

improve and, where necessary, develop systems to ensure records are accurate and timely, and that information shared across agencies is synchronized.

6.0 Criminal Justice Information Systems

In this section, I will discuss some successes that states have had in developing what are commonly known as Criminal Justice Information Systems (CJIS). Beyond imposing regulations on CDBs, it is incumbent on government to ensure that public records are accurate and timely at all levels in order to ensure their system can be rightfully referred to as an "authoritative source."

Following September 11th, there was a surge of interest in modernizing criminal justice information systems, making it easier for law enforcement agencies to share data quickly during investigations. (Chen et al, 2003; Morton, 2004; Zhao et al, 2006) A few states had already begun efforts to improve their technological infrastructure in their agencies dealing with courts, law enforcement and corrections. These efforts are important not only on the law enforcement and investigation side, but for millions of other people, more accurate and consistent data in the criminal justice system will mean that voting rights will be restored sooner and old convictions will not haunt them decades after they've reformed. Furthermore, people without a record won't be prevented from voting or getting a job because their name is similar to that of someone with a recent criminal record.

6.1 Colorado and the CICJIS

Colorado began its current project to modernize its criminal justice information systems in the early nineties, with the goal of developing a system that was "capable of

tracking the complete life cycle of a criminal case." (Report of the State Auditor, 2003) The resulting system, called the Colorado Integrated Criminal Justice Information System (CICJIS),[12] uses a hub architecture that links together the legacy systems of several state agencies, encompassing law enforcement, courts and corrections. CICJIS is notable for its success in improving record accuracy and has been the recipient of several awards from the Center for Digital Government and Government Technology Magazine.[13]

A central index stores summary information about individuals maintained by various agencies and points to more detailed records housed in the individual agencies' systems. Employees at each agency can, as authorized, query data stored in other agencies' systems. Crucially, the system is capable of event –driven data transfer, in which data that needs to be shared across agencies can be automatically transferred as soon as it enters the system at an individual agency. This type of information-sharing between agencies, in theory, should mean that everyone who needs it has the same data at essentially the same time, so if a data broker has a policy of verifying conviction information before sending out background reports, it should find the most timely information. Figure 1, below, shows a model of the system and the applications involved.

[12] The Colorado state government site for CICJIS http://www.state.co.us/cicjis/ offers an excellent overview of the system, including more detailed information about the architecture, standards, legacy systems and success measures.
[13] http://www.state.co.us/cicjis/ Mar 10, 2008

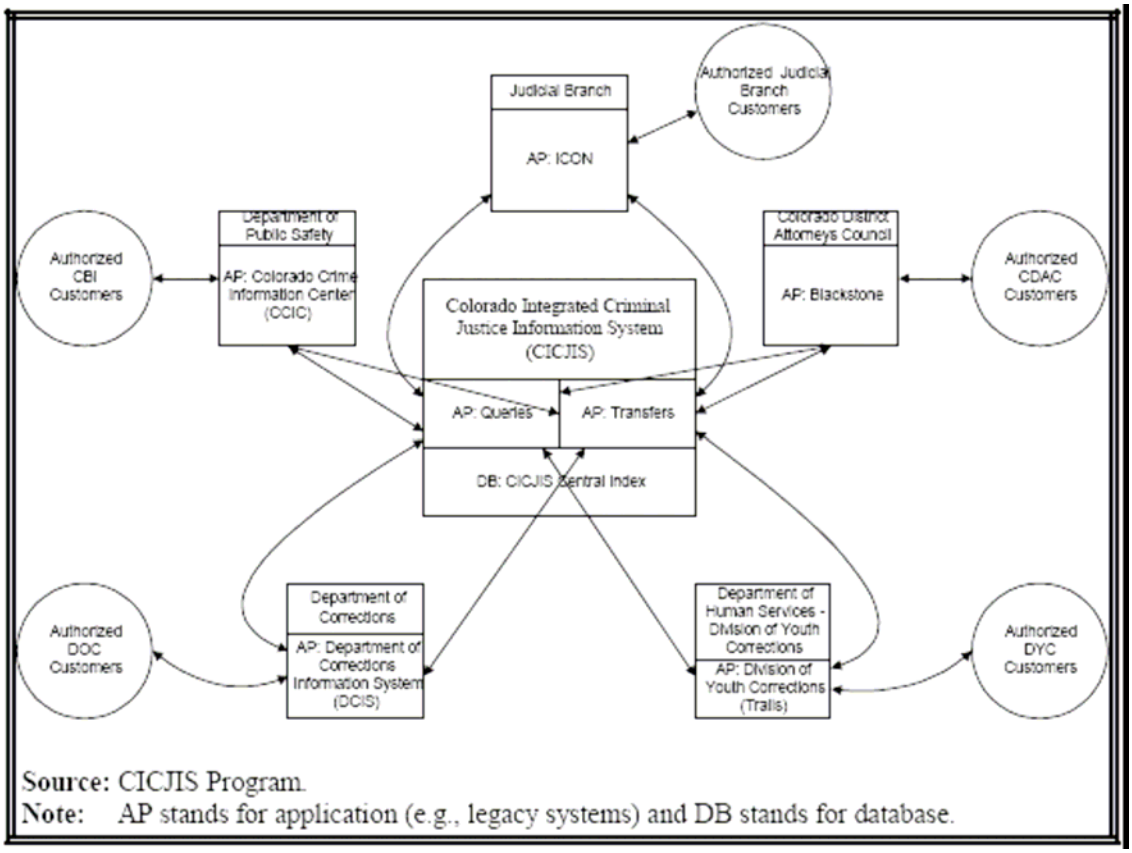

Figure 1: CICJIS System architecture. Source: Report of the Colorado State Auditor

An audit of CICJIS conducted in 2003 by the Colorado State Auditor tested the extent to which data between agencies matched. The report looked at the match rate of disposition records in different agencies linked through CICJIS, specifically, how often the disposition record in the Colorado Bureau of Investigation system, the Colorado Crime Information Center, agreed with the corresponding disposition record in an offenders' Records of Arrest and Prosecution in the Judicial branch. Before CICJIS was implemented, disposition records matched only eight to twelve percent of the time. In June 2003, three years after beginning to track match rates in CICJIS, 83 percent of records held in the two legacy systems matched, with a year-to-date match rate of 88.5%, having seen a steady increase over the period tracked. The most recent data available on

the state's website[14] indicates that the state-wide match rate for October 2006 was 93.24%.

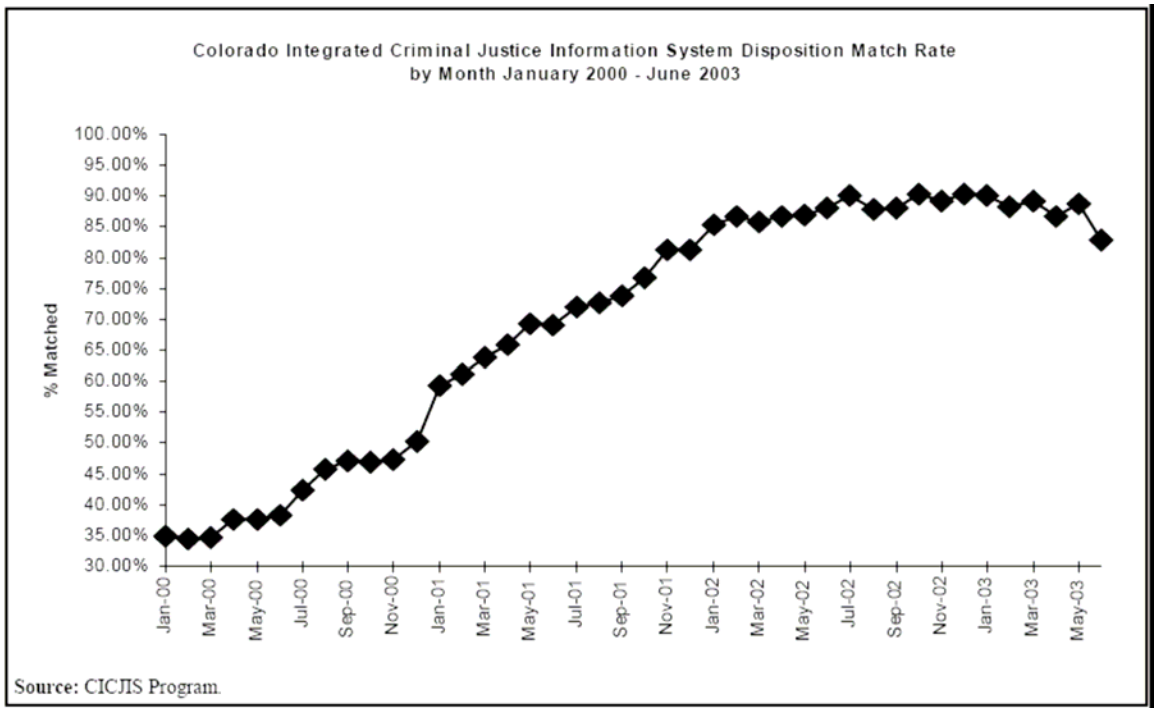

Figure 2: Disposition match rates in CICJIS. Source: Report of the Colorado State Auditor

These numbers illustrate dramatically the benefits for accuracy and data synchronization that a well-designed, well-funded criminal justice information system can have. The implications of these results for CDBs is that, wherever they get their data, it is much more likely that they will get accurate data and avoid harming consumers. Paired with legislation that establishes authoritative government sources for different types of public records, and after careful analysis of agency information practices and systems, CDBs should find it difficult to come across inaccurate information, and there would be little reason for not complying with the rest of the categories of provisions mentioned earlier when it comes to public records. Once a state's public records systems

[14] http://www.state.co.us/cicjis/DispoMatching/2006/10-2006/dispo_0610_summary.html

are integrated and held to a high standard, they may even be able to offer some of the services now offered by CDBs themselves.

7.0 Conclusion

Balancing access to public records so that the individual's right to privacy is protected, while the need for accurate information is met, is a complex issue. Employers have a legitimate interest in ensuring they do not hire people who might pose a risk to their business or the people it serves because of recent criminal behavior. But, those who have long reformed, or who were never found guilty of a crime in the first place, should not be penalized when seeking jobs they are qualified for. This balance can only be struck through a coordinated effort in which government provides the momentum for service improvements: first, by effectively regulating the ways that CDBs obtain, manage and provide access to personal information, and second by working to ensure that government agencies do the same, by evaluating and modernizing public records infrastructure.

Works Cited

Campbell, David. *Rules governing the use of background checks*. Crain's Cleveland Business, Small Business. Aug. 14, 2006

Chen, Hsinchun *COPLINK: Managing Law Enforcement Data and Knowledge*. Communications of the ACM 46:1, 2003

Colorado Integrated Criminal Justice Information System: Performance Audit. Report of the Colorado State Auditor. July 2003. http://www.leg.state.co.us/OSA/coauditor1.nsf/All/B9524355EC1566F687256E16005B1288/$FILE/1515%20CJIS%20Perf%20FY%2004.pdf

Fountain, Jane E. *Paradoxes of Public Sector Customer Service*. Governance 14:1, 2001

Glushko, Robert J. & Lindsay Tabas. *Bridging the "Front Stage" and "Back Stage" in Service System Design*. ISchool Report 2007-013. 2007 http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1013&context=ischool

Hoofnagle, Chris Jay. *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*. North Carolina Journal of International Law and Commercial Regulation Inc. Summer 2004

Laudon, Kenneth C. *Data Quality and Due Process in Large Interorganizational Record Systems*. Communications of the ACM 29:1, 1986

Laudon, Kenneth C. Dossier Society: Value Choices in the Design of National Information Systems. New York: Columbia UP, 1986

Morton, Heather. *Integrated Criminal Justice Information Systems*. National Conference of State Legislators. ed., 2004. http://www.ncsl.org/programs/lis/intjust/report01.htm

California Office of Privacy Protection. Feb. 13, 2007. http://www.privacy.ca.gov/lawenforcement/laws.htm

Colorado Integrated Criminal Justice Information System. May 10, 2006. http://www.state.co.us/cicjis/

Reed Elsevier Group. *Reed Elsevier to acquire ChoicePoint, Inc*. Press Release. Feb. 21, 2008. http://www.reed-elsevier.com/index.cfm?articleid=2200

Simpson, Glenn R. *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask Choicepoint – U.S. Agencies' Growing Use of Outside Data Suppliers Raises Privacy Concerns – A Fugitive Rents a Mailbox*. Wall Street Journal. New York, N.Y.: Apr. 13, 2001

Solove, Daniel J. *Access and Aggregation: Public Records, Privacy and the Constitution*. Minnesota Law Review 86, 2001-2002

Sullivan, Bob. *ChoicePoint files found riddled with errors: Data broker offers no easy way to fix mistakes, either*. MSNBC, March 8, 2005. http://www.msnbc.msn.com/id/7118767/

Teboul, J. *Services is Front-Stage*. Palgrave Macmillan, 2006

Tyworth, Michael & Steve Sawyer. *Organic Development: A Top-Down and Bottom-Up Approach to Design of Public Sector Information Systems*. 7th International Conference 'Human Choice and Computers', IFIP-TC9 'Relationship between Computers and Society', Maribor, Slovenia.

U.S. Dept. Of Justice V. Reporters Committee, 489 U.S. 749 (1989)

Zhao, J. Leon, et al. *Process-driven collaboration support for intra-agency crime analysis*. Decision Support Systems 41, 2006. 616-633