

Expanded Use of Criminal Records and Its Impact on Re-entry

**By: Sharon M. Dietrich, Managing Attorney
Community Legal Services, Inc., Philadelphia, PA**

**Presented to the American Bar Association Commission on Effective Criminal Sanctions
March 3, 2006**

Over the past decade, criminal records have become available and used for non-law enforcement purposes to an unprecedented extent. Several trends have dovetailed, with catastrophic effect for persons with criminal records (“PCRs”): (1) the availability to the public of criminal history record information has increased exponentially; (2) multitudes of civil legal disabilities have been created for PCRs, in crucial areas such as employment, public benefits, public housing and immigration; and (3) employers and landlords have chosen to broadly bar PCRs from jobs and housing in circumstances where they are not barred by law. Taken together, these trends are creating an environment in which even the most motivated ex-offenders cannot provide for themselves and their families, making them likely candidates for recidivism or permanent members of an underclass of Americans.

These developments raise questions about whether the availability of criminal record information can and should be curbed. Should criminal records be available on demand by any and every employer, landlord or nosey neighbor? Should they be available forever, or should there be a point at which they can be expunged or sealed? What should be done if they are not accurate? These questions and others are addressed in this paper.

Expanded Availability of Criminal History Record Information

A. What is a “criminal record”?

Any serious discussion about the availability of criminal history record information must begin with a recognition that there is no monolithic “criminal record” being examined by employers and others. Rather, criminal history record information is made available to the public through a variety of sources: state criminal record “central repositories” (often maintained by the State Police), the courts, private vendors which prepare reports from public sources, and even correctional institutions and police blotters.¹ When an employer or a landlord makes a decision on a “criminal record,” the

¹ SEARCH, the National Consortium for Justice Information and Statistics, Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information (2005) [hereinafter National Task Force Report on Commercial Sale of Criminal Record Information], at 22-26.

information could be obtained from any of these sources. Different laws and polices for the collection, use, and dissemination of criminal record information apply to each of these sources.²

B. What is the legal framework governing dissemination of criminal record information?

In the 1970s, the U.S. Department of Justice (“DOJ”) implemented regulations establishing minimum criteria for the handling of criminal history information by federally funded state and local criminal justice agencies (“the DOJ regulations”).³ These regulations led to virtually all states having passed legislation governing the dissemination of criminal records to some extent.⁴

With respect to the dissemination of records from the central repository, these state laws vary widely, from “open record” states in which records are readily available, to “closed record” states in which dissemination is closely regulated.⁵ By contrast, there has been a historical presumption of open access to court records.⁶ While commercial vendors may prepare criminal record reports from any publically available source, their primary source of information is the courts, because court records usually do not share the central repositories’ limitations on the availability of criminal record information.⁷

C. How do we know that criminal records have become more accessible?

There are numerous indicators that criminal records have become more available. One is because of the recent development of technology that has promoted accessibility (see the next section). Another is the increased percentage of non-criminal justice record checks reported by the Federal Bureau of Investigation (“the FBI”). From June 1, 2001 through May 31, 2002, noncriminal justice

² Robert R. Belair, Report of the National Task Force on Privacy, Technology, and Criminal Justice Information, NCJ 187669 (U.S. Department of Justice, Bureau of Justice Statistics, Aug. 2001)[hereinafter National Task Force on Privacy], at 1.

³ “Criminal Justice Information Systems Regulations,” 28 C.F.R. Part 20.

⁴ Paul L. Woodard and Eric C. Johnson, Compendium of State Privacy and Security Legislation: 2002 Overview, NJC 200030 (U.S. Department of Justice, Bureau of Justice Statistics, Nov. 2003) [hereinafter 2002 Compendium of State Privacy and Security Legislation], at 1. This publication cites and summarizes each state’s statute.

⁵ National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 1, at 40.

⁶ Id. at 45.

⁷ Id. at 22-23.

requests comprised more than half of the fingerprints submitted for processing, compared to around nine percent in 1993.⁸

Still another indicator is the burgeoning growth of the commercial sale industry. A recent report by the National Task Force on the Commercial Sale of Criminal Justice Record Information (“the National Task Force on Commercial Sale”) was the first comprehensive examination of the role of commercial vendors.⁹ Although the task force was unable to quantify the number of vendors or the checks they produced, it estimated that there are hundreds, maybe even thousands, of regional and local companies, in addition to several large industry players.¹⁰ Among the latter, the report noted that ChoicePoint conducted around 3.3 million background checks in 2002, most of which included a criminal record check.¹¹ USIS Transportation Services reported having 30,000 clients and processing more than 14 million reports per year.¹²

D. Why have criminal records become more accessible?

Notwithstanding statutory limitations on dissemination of criminal records, criminal history record information has, without doubt, become much more readily available over the last decade. Several factors have contributed to this trend, including the following.

1. Technology

Technology has played a major role. Automation of records and improvements in computing power have enhanced the compilation of criminal records.¹³ But among technological developments, the role of the Internet deserves particular scrutiny. According to a national task force report, “[T]he Internet greatly facilitates (and encourages) access to information for which the browser would not be inclined to make a trip to the courthouse.”¹⁴

In Pennsylvania, for instance, accessibility to records from both the Central Repository and the courts has been greatly facilitated by the Internet. In November 2002, the Pennsylvania State Police (“the PSP”) implemented its “PATCH system,” a mechanism for ordering a criminal record over the

⁸ 2002 Compendium of State Privacy and Security Legislation, supra note 4, at 9.

⁹ Id. at vi.

¹⁰ Id. at 7.

¹¹ Id.

¹² Id. at 8.

¹³ Id. at 29.

¹⁴ Id.

Internet. In the first year that the PATCH system was in operation, the PSP completed 567,209 background checks, up from 412,324 requests processed the previous year.¹⁵ At the PSP's budget hearing before the Senate Appropriations Committee in the spring of 2005, its Commissioner testified that the State Police had performed *1.7 million criminal record checks* in the prior year.

The Administrative Office of Pennsylvania Courts ("AOPC") is planning to make criminal record information even more readily available to the public. It has established a website on which the criminal court docket sheets from the entire state will be made available to anyone with Internet access who wishes to peruse them.¹⁶ Unlike a PSP record check through the Internet, the AOPC record check is nearly instantaneous and requires no fee.

Advocates have argued that AOPC's website will greatly increase the barriers already encountered by PCR's in Pennsylvania. The response has been that court records have always been publically available, so why should someone who wants to see them be forced to undergo the effort of traveling to the courthouse? The answer is in a concept known as "practical obscurity."¹⁷ The making of records available to the public at the courthouse balances public access with some privacy for PCR's, because it requires some effort to obtain the information. This balance is upset when information is available at the click of a computer mouse.

2. Safety demands in the post-September 11th environment

Without doubt, employers have become more security conscious since the attacks of September 11, 2001 and have turned to criminal record checks as part of their response.¹⁸ For instance, the commercial vendors reported significant increases in business immediately after September 11th, with ChoicePoint reporting a 30% increase and HireCheck reporting a 25% increase.¹⁹

¹⁵ Glenn May, "Online Background Checks Booming," Pittsburgh Tribune-Review (Nov. 30, 2003).

¹⁶ AOPC's website can be found at <http://ujportal.pacourts.us/WebDocketSheets/OtherCriteria.aspx>. Although it does not yet include every county in Pennsylvania – notably, Philadelphia County is not yet on line – the website is expected to do so by mid-year.

¹⁷ See the U.S. Supreme Court's decision in United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 780 (1989).

¹⁸ National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 1, at 31.

¹⁹ Id. at 32.

Employers confirm that criminal record checks have increasingly become a staple in their hiring processes. A member survey conducted by the Society for Human Resource Management in 2003 revealed that 80% of its organizations conduct criminal background checks, up from a 51% response rate in a 1996 survey.²⁰

3. New laws that exclude PCRs

In the past several years, federal legislation has been enacted that prohibits the employment of certain PCRs in numerous fields, such as hazmat drivers²¹ and aviation workers.²² The aviation checks alone required the screening of around 750,000 people.²³ The states have enacted a much larger number of occupational bars for PCRs, either through licensing or through prohibitions on hiring that are placed on employers. In Pennsylvania, 43 different occupations in which some PCRs are barred from working have been identified, from accountants through veterinarians.²⁴ These laws require large numbers of criminal background checks on potential employees.²⁵

4. Other reasons

Another reason often given for the increased demand for criminal record information is employers' desire to minimize risk and loss, whether by avoiding theft or by reducing the potential for negligent hiring lawsuits.²⁶

²⁰ Evren Esen, SHRM Workplace Violence Survey (Jan. 2004), at 19.

²¹ USA Patriot Act of 2001, 49 U.S.C. § 5103a.

²² Aviation and Transportation Security Act of 2001, 40 U.S.C. § 44963.

²³ 2002 Compendium of State Privacy and Security Legislation, *supra* note 4, at 9.

²⁴ Community Legal Services, Inc., Legal Remedies and Limitations on the Employment of Ex-Offenders in Pennsylvania (Oct. 2004).

²⁵ In addition, the application of these laws is not usually limited to those PCRs whose records contain prohibited convictions. In our experience representing clients in heavily regulated fields such as elder care and child care, employers required to conduct background checks frequently “over-apply” the laws, declining to approve people with any conviction at all.

²⁶ National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 1, at 35.

One can reasonably believe that concern about “bad public relations” also plays a role. News reports frequently blare that a certain employer or industry employs PCRs, as though the possibility is inconceivable.²⁷

Finally, it is worth noting what the National Task Force on Commercial Sale called “the bandwagon effect” – everyone else is conducting criminal background checks, and you fail to do so at your own peril.²⁸

Current Issues with Criminal History Record Information

A. Availability of nonconviction information

Outside of the criminal justice system, nonconviction information – that is, cases in which arrests have not led to convictions – is much less widely available than conviction information.²⁹ This distinction for dissemination purposes was codified in the DOJ regulations.³⁰ However, this distinction is threatened with erosion, as court records, which have been more likely to provide nonconviction information than central repository records, become more available through both technology and the proliferation of commercial vendors searching court records.³¹

Arrest records should not be considered by employers making hiring decisions. Because the use of arrest records as an absolute bar to employment has a disparate impact on African Americans and Hispanics, a rejection of a job applicant based on an arrest can constitute race discrimination in violation of Title VII of the Civil Rights Act of 1964 (“Title VII”). The enforcement guidance of the Equal Employment Opportunity Commission (“the EEOC”) on this subject states that “a blanket exclusion of people with arrest records will almost never withstand scrutiny.”³² Nevertheless,

²⁷ See, e.g., Sherri Ackerman, Felons Can Be Child Care Workers, Tampa Tribune (Dec. 18, 2005).

²⁸ National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 1, at 36.

²⁹ National Task Force on Privacy, *supra* note 2, at 20.

³⁰ 28 C.F.R. § 20.21. However, nonconviction information may be disseminated if permitted by officially promulgated policy. 28 C.F.R. § 20.21(b)(2).

³¹ National Task Force on Privacy, *supra* note 2, at 16 - 17 & n. 47, 80.

³² "Policy Guidance on the Consideration of Arrest Records in Employment Decisions under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. §§ 2000e et seq. (1982)" (Sept. 7, 1990), contained in Section 604 of the EEOC Compliance Manual, Vol. II.

employers would not be seeking out such nonconviction information if they did not intend to consider it.

The National Task Force on Privacy, Technology and Criminal Justice Information recommended that the distinction between conviction and nonconviction information be retained for non-criminal justice dissemination.³³ The task force noted that constitutional values, particularly the presumption of innocence, informed the policy behind providing more confidentiality and privacy to arrest records. When the Title VII implications are added, there clearly are reasons for nonconviction information to not be made available to the public.

B. Accuracy of criminal records

For the last decade, Community Legal Services, Inc. (“CLS”) has handled an active caseload of issues concerning the employment problems of PCRs. However, the last year or two has featured enormous growth in a related area: mistakes in criminal records that cause loss of employment, in many cases for people who have no criminal record at all. Clearly, the hysteria over criminal records has boiled over when even people without criminal records are precluded from jobs, raising serious questions about what is being accomplished by criminal background checking.

1. State laws governing accuracy

Although the DOJ regulations do not require enactment of state laws governing the accuracy and completeness of criminal records, all states and territories except the Virgin Islands had adopted such a statute by 1991.³⁴ Thirty-seven states require audits of the central repository.³⁵ All but two states have laws requiring procedures by which people can review their records and seek corrections of inaccuracies.³⁶

However, the existence of the state laws requiring access and review procedures does not necessarily mean that access and review actually is in place. For instance, Pennsylvania’s Criminal History Record Information Act specifically includes the courts within its definition of a “criminal justice agency” that is required to have an access and review procedure.³⁷ But our experience is that no such

³³ National Task Force on Privacy, supra note 2, at 80-81.

³⁴ 2002 Compendium of State Privacy and Security Legislation, supra note 4, at 5.

³⁵ Id. at 7.

³⁶ Id. at 4. The DOJ regulations require that individuals have the right to review their own records for accuracy and completeness. 28 C.F.R. § 20.21(g).

³⁷ 18 Pa. C.S.A. §§9102, 9104(a)(2).

procedure actually exists to correct court records; instead, one must hope to find a sympathetic court bureaucratic willing to make a change.

Nor does the existence of these procedures necessarily mean that criminal records are accurate. In the most recent audit of the criminal record system for Pennsylvania, the Office of the Attorney General of Pennsylvania determined that criminal court and Pennsylvania State Police records matched less than 80% of the time on data such as charges, name, date of birth, and social security number, and less than 70% of the time on disposition of the charges.³⁸

Moreover, an access and review procedure can come too late for someone who has been denied employment or housing based on a public record that is incorrect. CLS has seen cases where incorrect data entry has resulted in a listing of the wrong offense or the attribution of an offense to the wrong individual; where the same offense has been listed twice (making the record look like there were two offenses); and where the disposition of arrests has not been reported long after charges were dropped.

2. Criminal identity theft

Criminal identity theft is a particularly pernicious type of erroneous criminal record. It begins when a person who is arrested gives the name, date of birth, and/or social security number of another person. The person whose name and other information were fraudulently given to law enforcement (the “criminal identity theft victim”) then is linked with the criminal record of the arrests, convictions and bench warrants that belong to the person who was arrested (“the criminal identity thief”).

Criminal identity theft is not an uncommon occurrence. The primary criminal justice report examining this phenomenon estimated that 400,000 Americans were victimized by criminal identity theft in a year’s period.³⁹ CLS has assisted several dozen people with this problem. Philadelphia’s District Attorney’s Office indicates that they have advised around one hundred criminal identity theft victims over a seven year period.

In our experience, criminal identity theft can be devastating to its victims. Often, the people who caused the problem have extensive criminal records. Moreover, many of our clients work in occupations in which criminal record checks are required by law, such as long term care facilities, and the criminal identity theft rendered them virtually unemployable.

³⁸ Office of the Attorney General, Commonwealth of Pennsylvania, 2000-2001 Audit Report, Criminal History Record Information Act, Graph 15.

³⁹ Report of the BJS/SEARCH National Focus Group on Identity Theft Victimization and Criminal Record Repository Operations (Dec. 2005), at 2.

Unlike identity theft in the consumer context, criminal identity theft can be easily proved. Fingerprints generally are obtained when an arrest is made, so the fingerprints of the alleged criminal identity theft victim can be compared with those of the person who was arrested. Amazingly, though, very few central repositories or courts will correct the record of the victim even after criminal identity theft has been proved. The reason most often given is that the thief may use the victim's identity again when arrested, and expunging the record of the victim could put law enforcement personnel at risk or otherwise hinder law enforcement.⁴⁰

In our research of "best practices," CLS identified Virginia as the only state that expunges the record attributed to the criminal identity theft victim. We also learned through our investigation of this problem that very few states have adequate procedures to remedy criminal identity theft. Indeed, law enforcement is only beginning to grapple with effective solutions to this problem.⁴¹

CLS recently negotiated a pre-litigation settlement with the Pennsylvania State Police over this phenomenon, because the PSP did not sever the link between the record of the criminal identity theft victim and that of the criminal identity thief. Unless the victim's criminal record was sought by using a procedure unfamiliar to most employers, the PSP produced the record of the identity thief when a background check was done on a criminal identity theft victim. As a result of the settlement, the PSP will implement a technical solution in its database that allows "flagging" in the cases of established identity theft so that the identity thief's offenses will not be reported to the record of the victim.

A similar pre-litigation settlement implementing a software flagging system has been reached by public interest lawyers with the Michigan State Police. In Massachusetts, litigation is pending.⁴² Meanwhile, CLS has discovered that we need to also negotiate a solution or file suit against the Pennsylvania courts to correct their records where criminal identity theft has been proved, particularly as their website threatens to broadcast this misinformation over the "World Wide Web."

3. "False positives" and mismatches

Criminal records can also be erroneously reported because the search criteria of a database permit "false positives" – that is, a criminal record is attributed to someone who is not the person charged with the offenses. Among criminal record repository professionals, it is axiomatic that name searches for criminal records generally are disfavored, because fingerprint-based searches provide

⁴⁰ Id. at 8.

⁴¹ Id.

⁴² Bland v. Flynn, Secretary Executive Office of Public Safety, Massachusetts Superior Court SUCV2004-01751-F.

much more reliable matches between the person whose background is searched and the person with a criminal record.⁴³ However, criminal background checks by the public usually are name-based.

In name-based checks, the search criteria typically are some combination of name, date of birth, year of birth, and social security number. False positives are least likely to occur if the database requires a social security number for a match; more likely to occur if only a date of birth (and not a social security number) must be matched; and even more likely to occur if only the year of birth must match. Name-based checks in which only the names must match are extremely unreliable, yet such checks are done in many circumstances.

The most notable study on the reliability of name checks, conducted by a national task force to the U.S. Attorney General, found a 5.5% false positive result, and concluded that reliance on name checks alone would result in “large numbers of persons who do not have disqualifying criminal records [being] unfairly excluded from employment and other positions....”⁴⁴ Indeed, CLS has seen numerous cases where people have been denied work or fired based only upon a name match, such as a gentleman named Michael Jones who had the misfortune of sharing a name with a defendant in a large federal court drug conspiracy case.

Because of the potential for false positives, it is important for criminal justice information systems to provide enough information to permit an adequate match.⁴⁵ Nevertheless, there are public record systems in which inadequate match criteria are made available. For instance, the Michigan State Police require only year of birth for a match, resulting in numerous cases of “coincidences.” Similarly, the website of the Administrative Office of Pennsylvania Courts provides only a year of birth of the subject of the record.

⁴³ See, e.g., SEARCH, the National Consortium for Justice Information and Statistics and Queues Enforth Development, Inc., Interstate Identification Index Name Check Efficacy: Report of the National Task Force to the U.S. Attorney General (July 1999), at 6.

⁴⁴ Id. at 7-8.

⁴⁵ The National Task Force on Commercial Sale specifically addressed this issue:

The Task Force cautioned against the exclusion of identifiers from public records. The Task Force noted that, increasingly, changes in law restrict the inclusion of Social Security numbers and other identifiers in public records, including criminal history records. The Task Force believes that this trend will inevitably increase the risk that the wrong file will be associated with the wrong person. Moreover, the trend, if it persists, poses a threat not only to the quality of background checking, but also to efforts to prevent identification fraud.

National Task Force Report on Commercial Sale of Criminal Record Information, supra note 1, at vii; see also pages 15-19, 87.

4. Negligence by commercial vendors

Questions about the accuracy of criminal record reports prepared by commercial vendors have only recently begun to garner public attention, spurred in part by the report of the National Task Force on Commercial Sale.⁴⁶ CLS has seen this phenomenon directly, having handled numerous cases in which information that was accurately reported in court records for other persons was wrongly attributed by credit agencies to our clients. These cases include the following situations.

- ▶ A woman who had started the best job of her life was fired because a credit agency reported a drug offense by another woman of the same name, despite the fact that their dates of birth did not match.
- ▶ A commercial vendor confused twin siblings names Eric and Erica. Eric was in jail; Erica was fired from her job based on her brother's record. Needless to say, they shared the same date of birth; however, there were other (obvious) indicators that they were not the same person.

While some of the coincidences in these cases might make the commercial vendors' identification errors more understandable, these errors could have been cleared up if the employer and/or the commercial vendor had followed the law. Where a criminal record report is provided to an employer by a credit reporting agency, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*, is applicable.⁴⁷ Among the duties that FCRA imposes when an employer uses a consumer report of a criminal record provided by a commercial vendor for purposes of a hiring decision are the following.

- ▶ The employer must provide a clear written notice to the job applicant that it may obtain a consumer report. 15 U.S.C. § 1681b(b)(2). It also must obtain written authorization from the job applicant to get the report. 15 U.S.C. § 1681b(b)(3). Therefore, in situations where a commercial vendor is involved, the subject of the criminal record check ought to be made aware that a background check is being done, which often is not the case when criminal records are obtained directly by the employer from public sources.
- ▶ If the employer intends to take adverse action based on the consumer report, a copy of the report and a Federal Trade Commission ("FTC") Summary of Rights must be provided to the job applicant before the action is taken. 15 U.S.C. § 1681b(b)(3). The obvious reason

⁴⁶ See, e.g., John Christoffersen, Associated Press, Background Checks by Employers Spark Worries, Phila. Inquirer, Dec. 30, 2005; Matt Bradley, Who Is Checking the Background Checkers? Christian Science Monitor, Nov. 28, 2005.

⁴⁷ See Beaudette, FTC Informal Staff Opinion Letter, June 9, 1998 (available at <http://www.ftc.gov/os/statutes/fcra/beaudett.htm>).

for this requirement is to permit a job applicant to address the report before an employment decision is made.

- ▶ Afterwards, the employer, as a user of a consumer report, must notify the job applicant that an adverse decision was made as a result of the report and must provide, among other things, the name, address and telephone number of the credit agency and the right to dispute the accuracy or completeness of the report. 15 U.S.C. § 1681m(a).

Although these legal protections are well-established, they are often not followed. If they were, the clients described above should have been able to prevent their rejections based on the erroneous reports. Moreover, even PCRs whose records were accurately reported would have a chance to make their case as to why their criminal record should not disqualify them before they are turned away.

C. Completeness of criminal records - disposition reporting

The reporting of the disposition of pending charges can be very important to the person against whom the charges were brought. Even in cases where there has been a conviction, often the conviction will be on fewer than all of the original charges. Frequently, more serious charges have been dropped as part of a plea bargain. Disposition reporting is even more important to an individual against whom all charges were dropped. However, many charges contained in the central repositories have no disposition, whether because of policy or lengthy delays in reporting or entering the disposition.

The DOJ regulations establish minimum criteria for disposition reporting. To be “complete,” an arrest record must contain disposition information within 90 days of the disposition.⁴⁸ However, evaluations of disposition reporting suggest that this standard is routinely violated. According to a report prepared for the National Association of Professional Background Screeners (“NAPBS”), only 45% of 174 million arrest cycles have dispositions reported.⁴⁹

All but one state have enacted statutes establishing some form of disposition reporting requirements, but some of these statutes contain little to no particulars beyond a general reporting requirement.⁵⁰ Even the more detailed laws do not necessarily require reporting of all outcomes. For instance, only

⁴⁸ 28 C.F.R. § 20.21(a)(1).

⁴⁹ Craig N. Winston, The National Crime Information Center: A Review and Evaluation (Aug. 3, 2005) [hereinafter “The NCIC: A Review and Evaluation”], at 6.

⁵⁰ 2002 Compendium of State Privacy and Security Legislation, supra note 4, at 6.

33 states require notification of the central repository of a declination of prosecution.⁵¹ Only 31 states notify the repository if fingerprints have been submitted but no charges were filed.⁵²

In addition to policies that do not necessarily require that positive outcomes for the person who was arrested be reported, many arrestees are disadvantaged by delays in reporting outcomes.

- ▶ Although the average period between court disposition and notification of the central repository is 17.5 days, in many states it is significantly longer than average. At the outside, an average of 80 days is required in North Dakota for this communication to occur.⁵³
- ▶ An average of 29.5 days is needed to enter this information into the central repository database after it is received. As 24 of 39 reporting jurisdictions indicated that the information is entered in less than 10 days, other jurisdictions with much longer delays bring up the average. In Washington, data entry takes an astonishing 330 days.⁵⁴
- ▶ Twenty seven states reported that they have a backlog in entering disposition data.⁵⁵ The number of person-days needed to eliminate the backlog exceed a year in Hawaii (1,844 days), Indiana (444 days), Iowa (4,263 days), Mississippi (900 days), Nebraska (630 days), New Jersey (1,460 days), Ohio (1,000 days), Pennsylvania (867 days), and Washington (6,336 days).⁵⁶

Needless to say, expungements face these same delay obstacles even after being ordered by a court.

⁵¹ Id.

⁵² The NCIC: A Review and Evaluation, *supra* note 47, at 7. CLS has found this situation particularly difficult to rectify. To get the charges off of the State Police record, the person must have his fingerprints expunged. Because there is no underlying court case, the criminal justice players often are confused about why an expungement is needed.

⁵³ Sheila J. Barton, Survey of State Criminal History Information Systems, 2001, NCJ 200343 (U.S. Department of Justice, Bureau of Justice Statistics, Aug. 2003) [hereinafter “2001 Survey of State Criminal History Information Systems”], at 6.

⁵⁴ Id.

⁵⁵ Id.

⁵⁶ Id. at 37 (Table 13).

Recommendations

A. Access to criminal records should be limited.

1. *“Open access” policies by central repositories should be revisited.* Massachusetts provides a model for more restricted and thoughtful access. Its statute allows criminal record information to be provided to an employer through a “public access record check” only if the person is incarcerated or recently released. Otherwise, the employer must apply for a “special certification” that will be granted by a Criminal History Systems Board only if it determines by a two-thirds vote that the public interest in disseminating the information outweighs the person’s interest in privacy. There are exceptions for those who work with vulnerable populations such as health care patients, the elderly and children.⁵⁷

2. *The courts’ traditional open access to criminal records should also be revisited.* Given the huge growth of the commercial vendor industry, these records now are broadly available to their buyers, including nonconviction information that is much less likely to be available from the central repositories.

3. *Internet access to criminal history record information should be particularly discouraged.* Making criminal record information available on the Internet, especially immediately and at no cost, severely undermines re-entry goals by virtually eliminating any privacy for PCRs, no matter how old their records.

B. Expungements and sealing of convictions should be expanded.

4. *States should enact expungement and sealing laws.* Only 24 states purportedly have statutes that provide for the expungement of felony convictions, and in several cases, the circumstances in which expungement can be had are very restricted.⁵⁸ These mechanisms recognize that PCRs who have gone conviction free for a significant period of time should not forever have to bear the stigma and consequences of having a criminal record. The National Task Force on Privacy included among its recommendations that “criminal history record information should be sealed or expunged (purged) when the record no longer services an important public safety or other public policy interest.”⁵⁹

⁵⁷ Mass. Gen. Laws ch. 6, §§ 168, 172.

⁵⁸ 2001 Survey of State Criminal History Information Systems, *supra* note 51, at 4 & 29 (Table 9).

⁵⁹ National Task Force on Privacy, *supra* note 2, at 6.

C. Nondiscrimination laws should be passed and enforced.

5. *Existing Title VII protections must be enforced.* Although they are little known, some employment protections for PCRs do exist. Under federal law, the most commonly applicable employment protection is Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e *et seq.* Decisional law and policy statements of the EEOC have clearly established that employment discrimination against PCRs can have a racially disparate impact against African-Americans and Hispanics that violates Title VII.⁶⁰ However, this claim is little known and even less enforced. EEOC should improve its public education and enforcement efforts regarding Title VII violations against PCRs.

6. *States should enact nondiscrimination statutes.* Title VII does not protect all PCRs, most notably because its protections are limited to racial minorities. Thirty-three states already have complemented Title VII by enacting some form of nondiscrimination protection.⁶¹ The remainder should join them, so that PCRs do not continue to suffer the unfair consequences of the easy accessibility of criminal records.

D. Nonconviction information should not be made publically available.

7. *Information about arrests not leading to convictions should not be available to non-criminal justice requesters.* Given the constitutional presumption of innocence and employment law prohibitions against making hiring decisions based on arrests, this information should be sealed by both central repositories and courts.

E. Procedures for accuracy of criminal history record information must be implemented and strengthened.

8. *Criminal record repositories should implement procedures that permit easy challenge and correction of inaccuracies in the criminal records that they disseminate.*

9. *Every state should implement and publicize a sound procedure for correcting criminal identity theft.* The procedures soon to be implemented by the Pennsylvania and Michigan State Police could be looked to as models for states that continue to disseminate erroneous criminal

⁶⁰ The basic analysis of such a disparate impact claim is laid out in EEOC's "Policy Statement on the Issue of Conviction Records Under Title VII of the Civil Rights Act of 1964, as amended 42 U.S.C. §§ 2000e *et seq.* (1982)" (Feb. 4, 1987) ("the February, 1987 Statement"), which can be found in the EEOC Compliance Manual, Vol. II, Appendix 604-A.

⁶¹ Margaret Colgate Love, Relief from the Collateral Consequences of a Criminal Conviction: A State-By-State Resource Guide (The Sentencing Project, January 2006) (Chart 6), found at http://www.sentencingproject.org/rights_restoration/table6.html.

records for criminal identity theft victims. Alternatively, the state of Virginia's practice offers another alternative: expunge the record of the victim.

10. *Systems for conducting named-based criminal record checks should contain adequate safeguards so that false positives are avoided.* Date of birth and social security number should be mandatory search criteria. Never should "matches" be provided for solely a name match. Moreover, because false positives can be avoided in a fingerprint-based system, the FBI should continue to avoid providing name-based checks.

11. *The FTC should improve its public education and enforcement efforts concerning the Fair Credit Reporting Act.* FTC must step up to the plate to specifically address this issue, particularly given the typically severe consequences of an inaccurate criminal record. The burgeoning commercial vendor industry must be made to understand that negligence in preparing criminal background checks will cost them.

F. Dispositions must be reported in a timely fashion.

12. *All outcomes favorable to the person who was arrested should be reported to the central repository.* This includes declinations of prosecution and decisions not to charge a person after fingerprints were submitted.

13. *Central repositories with substantial backlogs in disposition reporting should be required by the Department of Justice to submit corrective action plans to eliminate the backlogs.* This will require the dedication of the resources necessary to enter the data.