August 5, 2005

Mr. Richard A. Hertling
Deputy Assistant Attorney General
Office of Legal Policy
4234 Robert F. Kennedy Building
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Re: Attorney General's Report to Congress on Criminal History Record Checks (OLP Docket No. 100)

Dear Mr. Hertling:

EPIC and the Privacy Rights Clearinghouse submit the following comments in response to the solicitation of the Attorney General for comments concerning non-criminal-justice background checks.[1]

The number of criminal background checks performed by employers has increased significantly over the past decade. As of January 2004, eighty percent of employers reported routinely conducting background checks on job applicants.[2] Currently, the FBI's Integrated Automated Fingerprint Identification System (IAFIS) holds 44 million digitized sets of fingerprints and processes an average of 60,000 prints per day.[3]

In response to the growing burden of performing these checks, the National Crime Prevention and Privacy Compact Council published an Interim Final Rule in December 2004, permitting the outsourcing of non-criminal justice background checks.[4] The FBI has the authority to share criminal history information with authorized state and local government agencies for official purposes, such as licensing and employment.[5] Until recently, requests for non-criminal background checks were filtered through state agencies that would check the prints against state criminal records before forwarding them to the FBI for analysis.[6] The States have also had the discretion to limit the occupations authorized for access to the IAFIS.[7] As part of this new policy, the Compact Council plans to authorize up to fifty private contractors to submit fingerprint applications directly to the IAFIS. Of these firms, some will act as "channelers" with direct access to the FBI's Criminal Justice Information Services (CJIS) wide area network, while others will be authorized recipients of Criminal History Record

[1] Criminal History Background Checks; Request for Comments, 70 Fed. Reg. 32849 (Jun. 6, 2005).
[2] Jon Bonné, *Most Firms Now Use Background Checks*, MSNBC, Jan. 21, 2004, *at* http://msnbc.msn.com/id/4018280/ (citing Society for Human Resource Management study).
[3] Gary Fields, *Ten-Digit Truth Check*, Wall Street Journal, June 7, 2005, at B1, *available at* http://online.wsj.com/article/0,,SB111810891957152558,00-search.html?KEYWORDS=background+checks&COLLECTION=wsjie/archive.
[4] Outsourcing of Noncriminal Justice Administrative Functions, 28 C.F.R. § 906 (2004).
[5] 28 U.S.C. § 534.
[6] *See* Fields.
[7] 28 C.F.R. § 20.21(c).

Information (CHRI) but not allowed to connect to the network.[8] The Compact Council also established standards for access, use, and dissemination of information acquired through this relationship.[9]

Congress has now directed the Attorney General to make further recommendations concerning:

> "improving, standardizing, and consolidating the existing statutory authorizations, programs, and procedures for the conduct of criminal history record checks for non-criminal justice purposes."[10] In preparing this report, the Attorney General has solicited public comment on fifteen factors to be considered in making the recommendations.

A number of issues must be accounted for in developing an outsourcing policy that protects individuals while expanding access to criminal records. Given the recent barrage of reported data breaches, coupled with the accuracy problems that seem to plague both IAFIS and commercial databases, the danger of allowing access to sensitive personal information is apparent.

This comment addresses the factors to be considered by the Attorney General and suggests policy recommendations, focusing specifically on the following issues:

- Safeguards to ensure that the information distributed to employer is accurate and does not include data that is beyond the scope of the investigation
- The numerous problems posed by supplementing national records with inaccurate information from commercial databases
- The need to impose time limits on the reporting of certain crimes in order to provide some level of social forgiveness
- Necessary measures to guarantee individuals the opportunity to dispute and correct reports

1. The effectiveness and efficiency of utilizing commercially available databases as a supplement to IAFIS criminal history information checks:

The effectiveness and efficiency of utilizing commercial databases will depend on several factors, many of which are tied to the standards that will govern the practice. The types of data involved, the methods for handling the data, the cost of the services, the accuracy of data, and the basic management of this process are just a few of the aspects that will determine the effectiveness and efficiency of the practice. Given the vague nature of this question, providing an informed and relevant answer is impossible.

[8] 69 F.R. 75,243 (Dec. 16, 2004).
[9] Security and Management Control Outsourcing Standards, 69 Fed. Reg. 75,350 (Dec. 16, 2004).
[10] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, 3759 (2004).

However, assuming this question is focused on supplementing IAFIS with criminal or personal history information present in commercial databases, we offer suggestions on whether to implement such procedures.

Under the FCRA, consumer-reporting agencies that provide information about an individual's criminal history that is "likely to have an adverse effect upon a consumers' ability to obtain employment . . . must maintain strict procedures" to ensure the accuracy of the information.[11] CRAs are required to make sure that the information they are providing is current *at the time of the report*.[12] Thus, relying on stored information as old as thirty days without verifying that the information is up to date does not meet this standard.[13]

Because of these requirements, increasingly companies are using non-FCRA databases for anti-fraud efforts and other purposes. And because these databases are not subject to the FCRA's accountability provisions, they are riddled with errors.

According to a study performed by Privacy Activism, 100% of participants found errors in their report provided by Choicepoint, ranging from incorrect addresses, phone numbers, and even social security numbers.[14] Moreover, a FOIA request for complaints to the FTC regarding commercial background checks revealed numerous instances if inaccurate reporting, ranging from wrong addresses or employment history to wrong social security numbers or criminal history information.[15]

The following are striking examples illustrating the problems of inaccurate background checks reported to Privacy Rights Clearinghouse:

- An individual from Montana reports on the problem of false hits: "I was notified by a company that I was hired by and to start March 1 that my FBI finger prints came back and there was a hit on them. To my SHOCK he told me the hit was first degree murder!!! And they were investigating me now. I told and tried to explain this was not true. Went to court house and police station and the only thing I could get was I had no criminal activity or record from 1976 until 2004. I faxed them the only thing I was able to get and tried to explain they can't give me a letter of dispensation on what happen when I was at one time held for questioning in as far as being a witness to a crime which was not first degree murder. The records of the court show nothing on this matter. I never went to court or made bond or had a trail. I think something has been done wrong but no matter who I talk with since this happened 18 years when I was [questioned] I am

[11] 15 U.S.C. § 1681k(2) (FCRA § 613).
[12] *Id.*
[13] *See* Allan, FTC Informal Staff Opinion Letter, May 5, 1999 (explaining that relying on database records that are updated every thirty days does not suffice to fulfill the requirements of FCRA § 613(2)).
[14] Privacy Activism, *Data Aggregators: A Study of Data Quality and Responsiveness*, May 18, 2005, *available at* http://www.privacyactivism.org/Item/222.
[15] Complaints to the Federal Trade Commission concerning background check companies obtained by the Privacy Rights Clearinghouse under the Freedom of Information Act (on file with author).

told that was too long ago, no records, no information and as far as me trying to get this corrected once they have my finger prints they will always have them?"[16]

- The following example illustrates the consequences of private firms failing to obtain updated information: "I was convicted of a misdemeanor crime, but it was dismissed through PC 1203.4. I applied and received an offer from Pacificare, but after a background search was conducted, Pacificare denied the offer based on information on the background search. The background search company (Acxiom) erroneously reported that I was convicted of a misdemeanor crime, and never dismissed. I complained to Acxiom, which then reinvestigated my files. They found that they did not do a thorough job, and provided me and [P]acificare with a corrected consumer report, which stated that I had no convictions. However, Pacificare decided that they were no longer interested in hiring me. I am currently unemployed because I put in my 2 week notice to my previous employer after receiving the offer from Pacificare. But now that Pacificare denied the offer, I do not have a job."[17]

- This California man investigated his own history to discover the source of chronic unemployment: "I saw CBS's Weekend Marketwatch & their story about employers doing background checks. This made me think that this could be why I have been unable to find employment for over a year. The firms that I send my resume to don't even call me back or spend the cost of a postage stamp. I went to the two firms mentioned in the news story: www.choicepoint.com & www.backgroundchecks.com & did a background check on myself. I would not hire me based upon what they told me about myself. Choicepoint has me down as having a Misdemea[n]or charge in Arizona. (Same name & birth date but different middle name). Backgroundcheck has me down with being charged with whole host of bad things across the bible belt states. (same name). What can I do . . . ?"[18]

An additional concern is the reporting of information stored in commercial databases that should not be available to the public. Because many states have set time limits on the reporting of criminal history information, controls must be implemented to ensure that state laws are followed in providing such records. Furthermore, once criminal information is trapped in a commercial database, without strict updating procedures in place, inaccurate records may not be corrected and distant convictions may not be disposed of properly. Most states limit access to authorized entities and then provide only conviction information, which in most cases prevents the release of off-limit records.[19] Measures must be implemented to ensure that commercial databases adhere to the limits set by states.

---

[16] From the files of the Privacy Rights Clearinghouse hotline.
[17] *Id.*
[18] *Id.*
[19] *See* Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information,* Aug. 2001, at 25.

2. Any security concerns created by the existence of these commercially available databases concerning their ability to provide sensitive information that is not readily available about law enforcement or intelligence officials, including their identity, residence, and financial status:

No formal safeguards are currently in place to prevent data brokers from revealing information about law enforcement officers. Some offer law enforcement officers the ability to opt out, but many officers have complained that data brokers do not comply with requests for opt out.

A recent San Francisco Chronicle article illustrated the ease by which protected identities may be obtained through commercial databases. Starting with the rumor that Joseph Wilson's wife may work for the CIA, within thirty minutes the author was able to obtain Valerie Wilson's maiden name (the name she used as an operative), address, supposed employer, and aerial photographs of her home.[20] This example clearly illustrates the danger posed to intelligence officials.

Limiting the scope of analysis to the safety concerns of law enforcement overlooks the importance of protecting other vulnerable groups. For example, victims of domestic violence, members of the judiciary, trial witnesses, and informants are not in a position to defend attacks, as they likely lack the training and resources to do so.

Accordingly, we urge the Attorney General to consider potential targets other than law enforcement and intelligence officials in making recommendations to protect the personal information of select groups.

5. Privacy rights and other employee protections, including:

A. Employee consent:

Employees must be fully informed of the process they are consenting to for consent to be meaningful. In addition, measures to ensure that use of an individual's prints are limited to the specific situation for which consent was given.

B. Access to the records used if employment was denied:

The opportunity for applicants to access records that prompt a denial of employment is not only an important aspect of a fair and informed practice but is essential to ensure the accuracy of personal information. Under the FCRA, if an employer plans on taking adverse action because of a consumer report, the employee must be provided a copy of the report prior to the action.[21] Allowing access to the files responsible for adverse actions provides employees with the opportunity to dispute information and potentially set the record straight.

---

[20] David Lazarus, *Privacy Is Easy To Breach*, San Francisco Chronicle, July 15, 2005, at C1.
[21] 15 U.S.C.S. § 1681b(b)(3).

Despite the FCRA provision requiring that reports be furnished to employees prior to adverse action, the likelihood of an individual being able to dispute and correct a report prior to adverse action is slim. In most cases, the hiring timeline does not allow for such administrative appeals and applicants are likely to miss out on potential job opportunities as a result. Considering the greater chance of flawed IAFIS records, the necessity of providing access and a chance to dispute the information is even more pressing than that for standard consumer reports.

Thus, the Attorney General should recommend stricter standards to govern this recent practice. In order to ensure that employees have a chance to comment on and dispute the report that dictates their future employment, a mandatory "use-and-challenge" provision must be implemented. This standard would allow employees to not only access, but also dispute, records *prior* to adverse action.

C. The disposition of the fingerprint submissions after the records are searched:

The destruction of fingerprint submissions following performance of background checks is essential to protect the privacy of individuals. Thus, we strongly encourage the Attorney General to recommend that current policy governing this process, defined in the *Security and Management Control Outsourcing Standards,* remains intact.[22]

By submitting fingerprints during the employment process, job applicants agree to allow a background check in that single instance, not to become part of a lasting database. Allowing retention of records after a check is performed serves no compelling purpose other than creating a national database that opens the door for non-consensual access to both fingerprints and the records associated with them. Retaining fingerprint records in order to allow ease of future checks on employees or notification of arrests is an unnecessary measure to remain informed on employee arrest and conviction data. Policies that require employees to report arrests to employers or submit to checks throughout their employment fulfill this goal without the invasion of privacy implicated by allowing retention of records.

Accordingly, we strongly urge the Attorney General to advise against the retention of fingerprint submissions upon completion of a background check and recommend measures to ensure the destruction of records.

D. An appeal mechanism:

Providing individuals with an appeal mechanism to dispute and correct criminal records is essential to ensuring accuracy and fair employment practices. Given the stakes involved in employee background checks, namely the employment and livelihood of individuals, allowing access and input on the personal information influencing employment decisions is an important measure for an effective process.

[22] 69 FR 75,350 § 7.02 (stating, "The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.).

Furthermore, the ability to appeal employment decisions and information present in records is necessary to protect the privacy of individuals. By submitting to such a check, an employee is allowing access to personal information otherwise limited to authorized entities. If employees are required to do so in order to obtain employment, they need a mechanism to ensure that the records revealed to others are, at the very least, accurate.

A process for appeal of employment decisions is also a necessary protection for employees. Without means to challenge employer use of criminal records, we risk encouraging disproportionate reliance on arrest data rather than balanced evaluation of employees and prospective employees.

Thus, we contend that the Attorney General should recommend an appeal mechanism that allows individuals to dispute and correct information prior to action by the employer. The opportunity to appeal should also extend to employment decisions made on the basis of background checks, in order to provide employees with remedies for misuse of information provided in these reports.

E. Penalties for misuse of the information:

We recommend that the Attorney General look to the FCRA provisions in suggesting penalties for misuse of criminal history information. Both civil and criminal penalties are available remedies for willful or negligent violation of the FCRA.

Upon proving willful violation, an individual may receive actual damages or statutory damages ranging from $100 to $1000.[23] In addition, punitive damages are available as allowed by the court.[24] Whereas actual damages are limited to an amount proven by the plaintiff to have suffered because of a willful FCRA violation, there is no upward limit on punitive damages. In cases where only negligence is proven, a consumer is able to recover actual damages.

The FCRA also provides criminal penalties for violation of two provisions: knowingly and willfully obtaining information on a consumer under false pretenses or knowingly and willfully providing information on an individual from the agency's files to a person not authorized to receive the information.[25] The penalty for either offense is a fine or imprisonment for no more than two years, or both.

F. Other privacy issues:

The privacy implications of expanding access to the FBI database are significant. Aside from the previously cited concerns, we would like to comment on additional privacy issues, including the handling of expunged and sealed records and the need to implement time limits for reporting of offenses.

[23] 15 U.S.C. § 1681n(a) (2005).
[24] 15 U.S.C. § 1681n(a)(2) (2005).
[25] 15 U.S.C. § 1681q-r (2005).

1. Expunged records and deferred adjudication

Our first concern is the potential for mishandling and reporting of expunged or sealed records. The process for expungement takes place on the state and county level, meaning that individuals rely on local agencies to carry out the requested destruction of criminal records.[26] However, expunged records that are unavailable through state databases may continue to be retained in the IAFIS and, therefore, available to CRAs with access to this database.[27] The expungement process is a key aspect of social forgiveness, in that it grants individuals the right to be absolved of certain crimes after an established period. In this sense, access to expunged records contradicts the social consensus regarding treatment of criminal histories.

Further problems arise in the case of deferred adjudication. At the discretion of the court or prosecutor, arrested individuals may have the option of serving a probation period in exchange for pleading guilty or no contest to the charges. Upon successful completion of the probationary period, the charges are dropped and no record of the conviction will result.[28] To prevent public access, an individual may have to petition for non-disclosure of the records. This situation is similar to that of expunged records—once the data is captured in the federal or commercial database, efforts to dispose of the history will likely be difficult if not impossible. Measures to ensure that these types of arrests are not reported as convictions and that no record of the arrest remains after the process for non-disclosure is complete are essential in protecting the privacy of individuals.

2. Time limits on reporting of criminal history information

Despite the 1998 amendment to the FCRA to eliminate time limits on the reporting of criminal convictions, many states continue to employ rules limiting the time for reporting. Allowing access to IAFIS will allow CRAs to circumvent state law by obtaining records through the federal database. Once these records make their way into a commercial database, the likelihood of an individual escaping the shadow of past mistakes is bleak.

In fact, reporting of crimes that exceed the time limits set by state rules is a selling point for many of these data brokerage firms. In a study of fifty randomly selected firms, 57%

---

[26] *See generally* Electronic Privacy Information Center, *Expungement*, *at* http://www.epic.org/privacy/expungement/ (explaining general process and requirements for expungement).

[27] Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology, and Criminal Justice Information*, Aug. 2001, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/rntfptcj.pdf, (stating, "Private databases may outflank State sealing and expungement laws. Once a criminal record has been captured in a private database or published in the newspaper (now also electronically searchable and available on the Internet) or published on the Internet, court or other legal directives to seal or expunge those records have limited effect.").

[28] Enter general definition of deferred adjudication.

reported the ability to search records dating back more than seven years.[29] In addition, several complaints have been issued to the FTC about this practice.[30] This is in clear conflict with state laws that impose time limits on the reporting of violations. Enabling private firms to access an additional database that may include older violations not accessible through state systems opens the door for the reporting of expunged or sealed records, violations for which the time has been served and should not be disclosed, and criminal records that are barred from reports under state laws.

The potential to create inescapable criminal histories will seriously impact, and possibly make it impossible, for individuals with distant convictions to secure meaningful employment. Accordingly, we urge the Attorney General to recommend setting time limits on reporting of criminal history information and employ standards to ensure that CRAs abide by these limits.

6. The scope and means of processing background checks for private employers utilizing data maintained by the Federal Bureau of Investigation that the Attorney General should be allowed to authorize in cases where the authority for such checks is not available at the State level:

In response to this factor, we urge the Attorney General to limit rather than expand the scope of authorization for private employers to access data maintained by the FBI.

In the absence of state authorization for such checks, private employers should not be allowed to bypass the State for direct access to the national database. Current procedures requiring state or independent agencies to process requests for national records are a necessary safeguard to protect individual privacy and ensure proper methods are used in obtaining and interpreting these records. Several reasons support this policy, including the potential for misinterpretation of records by unqualified employers, the potential for private employers to access information beyond the scope of their inquiry, and potential for employers to abuse this privilege.

States have established rules defining which occupations are allowed access to national records and the methods by which information represented in these records is evaluated and disseminated.[31] The types of offenses that disqualify an individual for employment depend on state or federal employment and licensing standards for a given occupation. Requiring state or independent agencies to evaluate records and make a "fitness determination" ensures that applicants are not discriminated against for irrelevant criminal histories or misinterpretation of a criminal record.

---

[29] Shauna Briggs, Meridith Tanner, Shawn Bushway, Faye Taxman, Mishelle Van Brakle, "Private Providers of Criminal History Records: Do You Get What You Pay For?" (Working paper prepared for forthcoming book, to be published by the Sage Foundation).

[30] Complaints to the Federal Trade Commission concerning background check companies obtained by the Privacy Rights Clearinghouse under the Freedom of Information Act (on file with author).

[31] *See* Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology, and Criminal Justice Information, Aug. 2001*, at 24-25.

Allowing private employers to bypass State regulations and access the national database opens the door for widespread abuse of current and potential employees. Because employers are not qualified to evaluate an FBI criminal record, the possibility that individuals will be unfairly categorized as criminals and, as such, unemployable is a likely scenario. Given the technical jargon that comprises these records and the high incidence of incomplete records, factual mistakes and uninformed decisions are very likely.

7. Any restrictions that should be placed on the ability of an employer to charge an employee or prospective employee for the cost associated with the background check:

Because of the impact of requiring employees to pay for background checks is grossly disproportionate to the burden placed on the employer and discriminates against low-income employees, we urge the Attorney General to recommend employers absorb the cost of performing background checks on employees and prospective employees.

Requiring job applicants and employees to bear the cost of background checks will seriously impact low-income individuals and place those in higher income brackets at an advantage in seeking and maintaining employment. Because the costs of obtaining and processing criminal background checks have the potential to be quite high, individuals seeking employment in certain sectors may be precluded from doing so merely because of the cost of the application procedure. For example, recent enactment of a fingerprint requirement in order to obtain a hazardous-materials license costs truck drivers an additional $94, aside from the $30-40 they already pay for a commercial drivers license.[32] For a person with sufficient income, fees may not be an issue, but for an unemployed job seeker any additional costs may pose a serious setback.

Moreover, allowing employers to charge applicants for background checks may result in prospective employees having to pay several different employers during the job search. This could create incentives for employees to purchase their own checks in order to show initiative by being prepared to hand one over at the request of employers. The cost to job seekers in these situations could be very significant and, in effect, hamper low-income individuals' ability to obtain work.

Along these same lines, safeguards need to be implemented to prevent employers from recovering the costs of background checks from employee wages, either directly or indirectly.

8. Which requirements should apply to the handling of incomplete records:

Given the high percentage of incomplete records in the FBI system, the Attorney General should recommend additional procedures to ensure the accuracy of reports and prevent improper handling of incomplete reports. These recommendations should include a

[32] Gary Fields, *Ten-Digit Truth Check*, Wall Street Journal, June 7, 2005, at B1.

provision affording employees and prospective employees the opportunity to evaluate and dispute records before adverse action is taken.

A number of situations may contribute to an incomplete record, including clerical errors, delays in updating of records, or arrests with no reported dispositions. Because the FBI system relies on states and prosecutors to provide updated criminal record information, inconsistencies in reporting have led to an incomplete database.[33] According to the Bureau of Justice Statistics, disposition reporting is very poor, averaging around 50%.[34] Furthermore, only half of misdemeanor acquittals are reported.[35] Given these statistics, the risk of a prospective employee being denied employment because of an incomplete record is staggering.

The best proposal to address these inadequacies, short of mandating consistent updating procedures for state and counties, is to impose strict standards on the private firms disseminating this information to employers. The FCRA requires that credit-reporting agencies verify that public record information is correct.[36] The FTC has deemed use of information stored in databases as much as 30 days old inadequate.[37] However, the numerous instances of inaccurate consumer reports illustrate a lack of vigilance on the part of commercial brokers.

Thus, measures must be implemented to ensure that commercial data brokers are vigilant in maintaining up to date information. Accordingly, we recommend that the Attorney General suggest strict limits on the dissemination of incomplete records.

9. The circumstances under which the criminal history information should be disseminated to the employer:

Because of the potential for abuse and stigmatization of individuals with criminal histories, we suggest the Attorney General recommend strict limits on information disseminated to employers.

Establishing uniform guidelines for the performance and treatment of background checks is important to ensure fair treatment of employees. In order to protect the privacy of prospective employees, dissemination of entire criminal records to employers should be limited. The current procedure employed by various states provides a model for this

---

[33] Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update*, at 86, Dec. 2001, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/umchri01.pdf.

[34] Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology, and Criminal Justice Information*, at 25, Aug. 2001, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/rntfptcj.pdf.

[35] BJS Technical Brief, at 2.

[36] 15 U.S.C. § 1681k (FCRA § 613) (requiring CRAs to "maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date").

[37] *See* Allan, FTC Informal Staff Opinion Letter, May 5, 1999 (explaining that relying on database records that are updated every thirty days does not suffice to fulfill the requirements of FCRA § 613(2)).

process. A standard that allows states to specify disqualifying crimes for a given occupation will provide employers with discretion over who they employ while protecting prospective employees from unfair hiring practices.

Allowing a state or approved independent agency to evaluate an individual's FBI record not only ensures that an informed decision will be made but also that employers will not improperly handle or use the information they obtain. These entities are best prepared to investigate gaps in records, such as arrests with no reported disposition, and make sure that state rules for time limits are followed.

14. The role that States should play:

States have the potential to play a very important role in this process. First, defining the occupations that will be authorized to access the national database for employment purposes should be left in the hands of the states. Second, states may be key in protecting the process against abuses by imposing time limits for reporting of criminal information and rules to govern treatment of expunged records. By establishing a policy that dictates which information is provided to employers and the ways in which this information is used, states may act as necessary arbiters of social forgiveness.

Accordingly, we urge the Attorney General to consider the potential impact that states may have on this process and refrain from contradicting state consensus regarding the use of criminal background checks.

Respectfully Submitted,

Chris Hoofnagle
Director
Electronic Privacy Information Center
West Coast Office

Tena Friery
Research Director
Privacy Rights Clearinghouse