

# Privacy Rights Clearinghouse

---

3100 – 5<sup>th</sup> Ave., Suite B  
San Diego, CA 92103

Voice: (619) 298-3396  
Fax: (619) 298-5681

E-mail: [bgivens@privacyrights.org](mailto:bgivens@privacyrights.org)  
Web: [www.privacyrights.org](http://www.privacyrights.org)

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  
Submitted electronically: [olpregs@usdoj.gov](mailto:olpregs@usdoj.gov)

**Re: Attorney General Report to Congress  
on Criminal Records and Employment Screening  
(OLP Docket No. 100)**

**Comments submitted by the Privacy Rights Clearinghouse  
and Privacy Activism**

Dear Mr. Hertling:

The Privacy Rights Clearing House (PRC)<sup>1</sup> and Privacy Activism (PA)<sup>2</sup> are pleased to offer the following comments on the Attorney General's pending recommendations to Congress relating to criminal records checks and employment.<sup>3</sup>

Our comments focus on three of the 15 factors for which the Department has solicited comment:

- Factor 1: the use of commercial databases
- Factor 5: privacy rights for employees
- Factor 6: access by private employers.

In addition to these comments, both the PRC and PA have joined the Electronic Privacy Information Center (EPIC) in more extensive comments. The PRC and PA also concur and fully endorse more extensive comments submitted by the National Employment Law Project.

---

<sup>1</sup> The Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy organization based in San Diego, CA, and established in 1992. The PRC advises consumers on a variety of informational privacy issues, including financial privacy, medical privacy, employment background checks, credit and identity theft, through a series of fact sheets as well as individual counseling available via telephone and e-mail. The PRC also represents consumers' interests in legislative and regulatory proceedings on the state and federal levels. [www.privacyrights.org](http://www.privacyrights.org)

<sup>2</sup> Privacy Activism is a nonprofit consumer education and advocacy group, established in San Francisco in 2002. It is particularly concerned with issues related to databases and data mining, including privacy, security, accuracy of information, and use of data for purposes other than which it was collected. [www.privacyactivism.org](http://www.privacyactivism.org)

<sup>3</sup> Request for public comment was published in the Federal Register, 70 Fed.Reg. 32849, June 6, 2005.

Our comments are organized as follows:

- 1. Introduction**
- 2. Commercial data bases – questions of accuracy**
- 3. Privacy rights and other employee protections, including ...**
  - a. Employee consent**
  - b. Access to records used if employment was denied**
  - c. The disposition of the fingerprint submissions after the records are searched**
  - d. An appeal mechanism**
- 4. Access by private employers**
- 5. What consumers tell the PRC about employment background checks**

## **1. Introduction.**

The Intelligence Report and Terrorism Prevention Act of 2004 [Pub.L. 108-458] requires the Attorney General (AG) and the Department of Justice (DOJ or Department) to recommend ways to Congress for improving, standardizing and consolidating the existing statutory authorization, programs, and procedures for the conduct of criminal history record checks for non-criminal justice purposes, primarily employment purposes. The Department now solicits comment on 15 factors to be considered in making recommendations.

Terrorist threats, workplace violence, and reported abuse of vulnerable segments of the population have contributed to a dramatic increase in criminal records checks. Advances in technology have also made criminal history checks faster, less expensive, and easy to obtain from a variety of sources.

The Society for Human Resource Management (SHRM), [www.shrm.org](http://www.shrm.org), reported in 2003 that 80% of private employers now conduct criminal background checks.<sup>4</sup> Add to this the requirement for criminal checks for public sector employees as well as numerous state and federal laws that require criminal background checks for certain categories of work. The result is that an applicant for nearly any job will face a criminal background check. For many jobs, access to national data files is already allowed by state or federal laws.<sup>5</sup>

Private sector job applicants and employees are given some rights under the federal Fair Credit Reporting Act, 15 USC §1681 et seq. (FCRA). The FCRA imposes obligations primarily on third-party screening companies, called consumer reporting agencies under the law. The FCRA also imposes some additional obligations on employers, called “users” of employment consumer reports.

---

<sup>4</sup> “Most firms now use background checks, Survey: 8 in 10 probe criminal history amid security worries,” January 21, 2004, by Jon Bonne, MSNBC.com, [www.msnbc.msn.com/id/4018280/](http://www.msnbc.msn.com/id/4018280/)

<sup>5</sup> For example, National Child Protection Act of 1993, 42 USC 5119a.

Private employers generally do not have access to the national FBI crime data base. Instead, a criminal history check for private employment is usually conducted through acquired public records maintained by commercial data vendors.

Before allowing greater access by private employers and commercial data brokers to DOJ criminal history files, the Department should consider existing problems encountered by individuals seeking work in the private marketplace. (For real-life stories, see section 5 below.) The FCRA currently offers national standards for employees and job applicants. However, the FCRA still has many shortcomings which should not be incorporated into any federal program to grant access to private employers and commercial data vendors.

As we discuss further, existing problems in the employment screening process — particularly with accuracy — can lead to chronic unemployment or dismissal from a longstanding job. The job applicant or employee has virtually no rights to have an adverse decision reconsidered, even when decisions are based on inaccurate information. Any standards for access by private employers and commercial data vendors must go beyond the current requirements of the FCRA.

## **2. Commercial data bases – questions of accuracy (Factor 1)**

Adverse effects of inaccurate data are most often studied and reported in the context of credit reports. Reports on accuracy of credit information have been issued by two national consumer organizations,<sup>6</sup> and the subject is currently under study by the Federal Trade Commission (FTC).

Similar scrutiny is needed for commercial data vendors that collect and report criminal history information for employment or other purposes. This is especially true because vendors disclaim responsibility for the accuracy of information contained in public records, including criminal records, which they acquire and sell. We believe the effectiveness of using information from commercial databases is questionable because the accuracy of the data itself is questionable.

We base this assessment in part on a study PrivacyActivism released in May 2005<sup>7</sup> of ChoicePoint employee background checks and ChoicePoint and Acxiom consumer reports<sup>8</sup>. Because of difficulties in obtaining employee background checks in compliance with the Fair Credit Reporting Act (FCRA<sup>9</sup>), the sample analyzed is small — only 11 people participated in

---

<sup>6</sup> *Mistakes Do Happen: A Look at Errors in Consumer Credit Reports*, <http://uspirg.org/uspirg.asp?id2=13649&id3=USPIRG&> and *Credit Score Accuracy and Implications for Consumers*, (CFA, December, 2004) [www.consumerfed.org/121702CFA\\_NCRA\\_Credit\\_Score\\_Report\\_Final.pdf](http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf)

<sup>7</sup> The entire study may be viewed online at <http://www.privacyactivism.org/DataAggregatorsStudy>.

<sup>8</sup> Employee background checks are regulated by the Fair Credit Reporting Act (FCRA). Data brokers that sell them are legally bound to provide background check information only to qualified employers. Some companies give individuals who provide sufficient personally identifying information the ability to purchase their own consumer reports. Since the ChoicePoint security breaches that came to the public's attention in February 2005, that company now offers public records reports to individuals at no charge.

<sup>9</sup> FCRA Sec. 603(h) limits the use of employee background checks to employment purposes: "The term 'employment purposes' when used in connection with a consumer report means a report used for the purpose of

the study. The results, however, are startling, and call for a larger-scale study, certainly before the DOJ considers giving some commercial data brokers direct access to the FBI's Criminal Justice Information Services (CJIS) wide area network, and allowing others to receive Criminal History Record Information (CHRI) (although not allowing them to connect to the network).

The PrivacyActivism study found that *all* the ChoicePoint background checks that participants in the study received contained at least one error. The study broke down the error types in the following way:

- 73% of participants (8 out of 11) had errors in their biographical data.
- 25% of the biographical data (15 out of 61 items) in the participants' reports was incorrect. (Biographical data is name, current address, Social Security number, date of birth, and phone number.)<sup>10</sup>

These basic biographical errors raise the strong likelihood of misidentification and of individuals being wrongly connected with criminal records. A background check system that holds the potential for serious, consequential errors based on the inaccuracy of the data obtained for employment screening cannot be considered either effective or efficient.

**Recommendation:** Before the DOJ considers outsourcing non-criminal justice background checks to commercial data brokers, we suggest it conduct a test for accuracy by ordering background checks for a sampling of 50 to 100 of its own employees, and having them tabulate and analyze the errors they find.

### **3. Privacy rights and other employee protections, including ... (Factor 5)**

#### **a. Employee consent**

Certainly no job applicant or current employee should be investigated for routine screening without informed consent. Employee notice and consent to a criminal background check are fundamental privacy rights. However, consent alone is not enough to ensure privacy rights. This is simply because the applicant or employee has no real choice but to give consent if such is the requirement set for the job.

The FCRA requires notice and consent to be provided on a document separate from other documents such as the job application form. If the Department is to allow private employers and commercial data vendors access to DOJ databases, employee privacy is only effective if the Department adopts standards that go beyond the FCRA.

For example, along with notice and consent, an employee whose criminal history is accessed should also be given notice of the nature and scope of the background check as well as the

---

evaluating a consumer for employment, promotion, reassignment or retention as an employee.”

<sup>10</sup> Acxiom's consumer reports, of which only six of eleven requested were ever received, showed a 13% error rate for biographical information.

federal data file that will be searched.<sup>11</sup> The notice should also tell the subject whether the background check will be conducted solely through fingerprints or if, absent available fingerprints, other identifiers such as name, date and place of birth, Social Security number, address or other information will be used.

The job applicant should also be given the opportunity to preview negative information that is likely to threaten a job prospect. The opportunity to review adverse data should come *before* the information is provided to an employer or other decision maker. The subject's ability to identify problems *before* an adverse decision is reached is fundamentally fair given variance in state reporting requirements as well as serious concerns about the completeness and accuracy of data reported to the federal repository.

Companies that furnish public record information for employment purposes are required by the FCRA to either (1) notify the consumer of adverse information, or (2) adopt strict procedures to ensure public record information is current at the time a report is made to an employer. (FCRA, §613, 15 USC §1681k) The DOJ should adopt the standard of advance notice in all instances.<sup>12</sup>

Any number of situations can adversely affect a job applicant or even result in the termination of a long-time employee in good standing. We at the PRC are struck by some of the disheartening stories we hear from consumers who call our hotline or contact us online (see section 5 below for actual stories). Here are just some of the things that *can and do* happen:

- State criminal records report an arrest but not the case disposition.
- Court records are inaccurate.
- The subject is the victim of identity theft.
- The person's name appears as an alias in court records even when a mistake has been corrected.
- A criminal conviction is reported even though a period of probation or deferred adjudication was served with the understanding that a conviction would not result.
- Convictions that are expunged or records believed sealed appear on background check reports.

We elaborate on real-life problems encountered by people who contact the PRC and from media reports in Part 5 of these comments.<sup>13</sup>

---

<sup>11</sup> The National Criminal Information Center, for example, includes not only information on criminals and criminal offenses but also, among other things, data about stolen property and missing persons. <http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm>

<sup>12</sup> To our knowledge, ChoicePoint is the only consumer reporting agency to publicly state a policy of notifying consumers directly of adverse public record information. This statement came only after ChoicePoint's widely publicized data breach in early 2005. <http://wired-vig.wired.com/news/privacy/0,1848,67276,00.html>

<sup>13</sup> Similar problems and concerns are addressed in a report entitled *The National Crime Information Center, A Review and Report*, prepared by Assistant Professor Craig N. Winston for the National Association of Professional Background Screeners. [www.napbs.com/MiscDocs/NCICReportJuly252005.pdf](http://www.napbs.com/MiscDocs/NCICReportJuly252005.pdf)

#### **b. Access to records used if employment was denied**

Fairness dictates that subjects always be given access to records and reports of employment background investigations whether employment is denied or not. This is a significant shortcoming of the FCRA and one that should not be incorporated into standards set for private access to DOJ databases.

Under the FCRA, an employer is required to provide a copy of the report when there is an “adverse decision,” that is when the employer does not hire a prospective employee or decides to fire a current employee. This standard is essentially unworkable and unenforceable, particularly when it relates to pre-employment checks. An employer has only to say that a more qualified applicant was hired. This essentially forecloses the applicant’s ability to find out if anything in the report was inaccurate or incomplete. Without an absolute right to find out what is in his or her report, negative and inaccurate information can follow one for a lifetime.

#### **c. The disposition of the fingerprint submissions after the records are searched**

The only valid reason to maintain fingerprint submissions is to verify the accuracy of data file searches. Even this purpose should have a time limit for when searches must be verified. Presumably most of the searches will result in a “no hit,” that is, a law-abiding citizen’s fingerprints are routed to federal criminal authorities for purposes of a routine employment background check.

It would be inappropriate for the Department to incorporate fingerprints of law-abiding citizens into the IAFIS [Integrated Automated Fingerprint Identification System]. Currently, such fingerprints are destroyed once results have been reported. The federal government should retain this practice. We urge the Department not to be influenced by states that retain fingerprints after initial, routine employment screening.

A nationwide data file of fingerprints submitted by law-abiding citizens raises serious privacy and due process concerns. Under such a system, one arrested but never convicted could face loss of a long-time job. Sufficient procedures are already in place to allow employers to periodically review a worker’s background, including criminal records checks. Some jobs require employees to report an incident.

For the government to maintain a permanent file of submitted fingerprints raises the possibility that at some time the fingerprints will be used for a secondary purpose that has no bearing on the original purpose for which the prints were submitted. Such use would violate basic Privacy Act principles prohibiting secret files as well as secondary uses of collected data.

#### **d. An appeal mechanism**

Shortcomings in the current process for screening by private employers illustrate that job applicants and employees must have some means to “clear” their name when erroneous or incomplete information is provided to a private employer. Subjects, under the FCRA, may file a dispute with the consumer reporting agency that compiled and furnished the information.



However, while the dispute is being investigated, the employer is likely to go ahead and hire someone else. Even if the problem is ultimately corrected, the employer is under no obligation to reconsider an adverse decision or reinstate a withdrawn job offer.

In reality, for employers hiring in today's atmosphere of suspicion, any "hit" coming from a criminal data file is enough to block an applicant's job prospect. As we discuss in parts 2 and 5, databases can and do produce false results. Many situations can lead to a false "hit."

Inconsistency in state criminal records and failure to record a case's resolution can also harm an individual's job prospects. Even when information is accurate, the employer, under the FCRA, does not have to consider the relevancy or age of an offense, or an individual's work history.

To ensure individual privacy and integrity of information, an appeal mechanism is needed. An individual should always be able to *dispute* inaccurate and incomplete information provided by a data vendor. In addition, it is essential that individuals be given a means of *appeal* that requires an employer to reconsider a decision based on faulty information.

#### **4. Access by private employers (Factor 6)**

Most individuals seeking employment today will undergo a criminal background check. The means for conducting such checks vary greatly. It is most unlikely that an employer in this day and age of online access to criminal history information will visit the local courthouse to search for criminal records information. Rather, employers want access to — and many jobs now require — a national criminal records check. For this, a private employer may use an Internet look-up site or, more likely, hire a third party screening company.

Criminal records are then searched by matching one or more data points such as name, date and place of birth, address, and/or Social Security number. Fingerprinting is a more reliable, but still far from foolproof, means of matching an individual with a criminal case. This is the means of access most commonly used to check state and federal data files.

Private employers do not have direct access to the FBI's criminal data files. Still, over half the FBI's fingerprint checks are now employment related, amounting to 9 million checks for private employers in 2004.<sup>14</sup>

The use of private data vendors for national criminal screening inevitably leads to vendors in the business of collecting, maintaining and distributing fingerprints. Given the history of this industry with data accuracy and security, the Department must establish and enforce strict standards to ensure the integrity of this process, along with substantive penalties, including contract termination, for intentional or negligent breach of these standards.

One fingerprint standard we would recommend for private vendors who supply fingerprints is that no fingerprints more than 18 months old should be accepted and that any older commercially obtained fingerprints retained by the FBI, if it does retain them, should be destroyed. It is well

---

<sup>14</sup> *Job Seekers Increasingly Fingerprinted*, Gary Fields, The Wall Street Journal (June 13, 2005), [www.privacy.org/archives/2005\\_06.html](http://www.privacy.org/archives/2005_06.html)

known that fingerprints change over time and that they may change dramatically, depending on an individual's occupation.

## **5. What consumers tell the PRC about employment background checks**

Based on our experience and the problems reported to us by individuals who have had background checks conducted, we believe employment background screening is an emerging public policy issue deserving substantial analysis and debate. As such, it should be entitled to far broader and more open public scrutiny than it will receive during this comments process where a limited number of interested parties submit comments in response to a *Federal Register* notice.

We offer the following information in the spirit of expanding the discourse about employment background screening.

The PRC has developed three educational guides about employment background checks.

- *Employment Background Checks: A Jobseeker's Guide*, <http://www.privacyrights.org/fs/fs16-bck.htm>
- *Employment Background Checks in California: New Focus on Accuracy*, <http://www.privacyrights.org/fs/fs16a-califbck.htm>
- *Employment Background Checks: A Guide for Small Business Owners*, <http://www.privacyrights.org/fs/fs16b-smallbus.htm>

In addition, the PRC maintains a consumer hotline and online inquiry/complaint form through which consumers can voice opinions, relay privacy problems, and complain about various instances involving the misuse of their personal information. Inquiries, questions, and complaints about background checks have increased dramatically over the last few years, coinciding, we believe, with the great increase in the number of employment background checks now being conducted. Interest in the PRC's educational materials regarding employment background checks has shown a similar increase

For example, until recently identity theft was the top reason the public contacted the PRC or accessed our educational materials online. Now, with approximately 120,000 unique visitors to our web site each month, the number of "hits" to our employment screening web pages nearly equals the "hits" on our identity theft pages. In addition, of the nearly 100 hotline and e-mail inquiries answered by PRC staff every week, questions about and reports of serious problems with employment background checks is a top reason for contact.

The following real-life examples illustrate the need for the Department to create and enforce strict standards of accuracy, privacy, and procedural rights before expanding access to national criminal data files. In most of the situations reported below, the employment background checks were conducted by third-party screening companies subject to the FCRA. Although conducted within this regulated environment, serious mistakes were nonetheless made. The subject — the person who was the *victim* of an inaccurate or incomplete background check — was then left to "clean up the mess."

**In the cases reported below, names and other details have been changed or omitted, except**



**in the first case reported, which is part of public record.**

**False information reported.** Mr. Socorro was fired from his executive-level position with Hilton Hotels after a background check returned a false positive. Mr. Socorro never got his job back, despite the fact that he was able to clear his name. Mr. Socorro's problems didn't stop there. He has had trouble getting a job for several years after his bad background check incident. (Edward Socorro, Plaintiff, vs. IMI Data Search, Inc. and Hilton Hotels Corp., Defendants. Case No. 02 C 8120, United States District Court for the Northern District of Illinois, Eastern Division, 2003 U.S. Dist. Lexis 7400, April 28, 2003, Decided; May 2, 2003, Docketed)

**False information reported.** A 49-year old engineer was fired from his job because a background check report said there was an outstanding warrant for his arrest. After many hours spent trying to find the source of this inaccurate information, he learned a background checking company had confused him with a much younger man with a similar name but of a different race. The background checking company refused to change its report; the court refused to change the file because the record did not belong to the engineer; and the employer refused to take him back because it sensed trouble. The best this victim could do was to obtain a letter, which he must carry with him at all times, from the state Attorney General saying there is no outstanding warrant for his arrest.

**No access to report.** A young father from a mid-Western state secured a badly needed job. He was fired after a short time with only the vague explanation that there was something "wrong" with his background check. Not having seen the report, he could only guess that the "problem" may have been from a minor offense for which he was offered and completed a period of probation with the understanding that a recorded conviction would not result. When advised of his rights by PRC staff to see his report, this individual received a copy of the report from the employer and was rehired.

**False information reported.** An applicant at a major department store chain was not hired for a job because a national background screening company mixed his identifying information with that of another person. Even when the mistake was reported, the chain withdrew its job offer.

**Identity theft victim.** Karen first learned she was a victim of criminal identity theft when she couldn't get a job or rent an apartment. She has been unable to resolve the matter and regain her good name, even after visiting several police departments in jurisdictions where her imposter was arrested.

**Identity theft victim.** Tina had a background check done for a job she was applying for at a southern university. The report included nine pages detailing criminal activity. She believes her sister stole her identity. She has been frustrated in her efforts to take care of the problem because she has been unable to get the cooperation of either the AG's office or law enforcement to help her clean up her record.

**Following are the largely unedited first-person excerpts from e-mails send to the PRC:**

**03/05, TX.** ChoicePoint got obviously incorrect information on me from the Texas Department of Public Safety and embellished on it. They turned a simple 30 year old misdemeanor into a felony conviction with me having served 7 years which made me look like a paroled convict. I was convicted of a misdemeanor 30 years ago. Company X did a background check and ChoicePoint, Inc. told them I had a felony I had served seven years for. They bought that info from the Texas Department of Public Safety. They didn't even have my name correct. They were giving out what I was charged with not what I was convicted of. Company Y did an earlier check and would not hire me either. Since 9/11 everyone is doing background checks. No telling how many jobs these people have cost me. In 2000 I was a Quality Control inspector responsible for over a \$40 million dollar project in the electrical engineering department at a local chemical plant! Now I'm not fit to sell wire nuts to the public at Company X!<sup>15</sup>

I have proudly served my country and have two Honorable Discharges and a service citation. I have been the leader of a civic group in my home town for four years but Company Y won't let me sell light bulbs to the public. I've been unemployed for 9 months!

**08/03, MO.** I am currently listed as an 11 times convicted probation violator and have never been on probation a day in my life. And the records came to federated dept. stores from a background check they conducted from an Internet company I was promptly removed from there employ. As I dug into this error. I met with the records chief for the city/county of X and his response was that these were times I was late making court payments and the "syntax" was such that that was how it got entered. [W]ell the payments were on traffic tickets. Well on the background check it said it didn't include traffic offences...so I asked for a signed letter that I was never indeed on probation and was told I would need to hire a lawyer to get any change or correction completed.

**06/04, no location.** I was just terminated from my job because I didn't tell them I had a conviction 36 years ago. This conviction was non-violent or non-drug or sex-related and had nothing to do with my work.

**01/04, TX.** The following is the letter I sent to Company T: *Attention: T Personnel Department Dear Sirs, I recently applied for employment at the new T Memorial City Mall store in Houston, Texas. As part of that application and interview process, I authorized T to perform a background check on me. A few days later I got a telephone call from a local employee telling that my application was declined because I failed the background check. I was TOTALLY SHOCKED and completely DISMAYED!! I've never been arrested in my life and haven't had so much as a parking ticket in more than 20 YEARS! Shortly thereafter, I also received a letter from you (T) which included a copy of that background report. If anyone in your office had taken the time to actually look at the report they could have easily seen that it is completely FALSE and incorrect! The person shown on the report has different middle name from mine and has a completely different date of birth. ITS NOT ME!! In fact, the report even states that VERIFICATION IS REQUIRED by the receiver! I've contacted Secure Point (the company that provided the report to T) and have vigorously disputed the report and have told them to purge my file of this*

---

<sup>15</sup> See, "Bad Data Fouls Background Checks," by Kim Zetter, *Wired*, March 11, 2005, [www.wired.com/news/privacy/0,1848,66856,00.html](http://www.wired.com/news/privacy/0,1848,66856,00.html)

*completely false and highly damaging information that they have associated with my VERY GOOD name.*

*Now, I want T to also completely destroy all printed copies of this report that it may have [in] their files and to purge all electronic, and email versions of it as well. I would certainly appreciate it if someone from the Personnel office would please call me so that I can confirm that this request will be carried out immediately and thoroughly! (No name)*

Today, I received letters from both Secure Point and T. Secure Point wrote to explain that my dispute to their report was in fact correct and that they have amended the report "to reflect that I was no longer a FELON!" and that they had forwarded the amended report to T. T also wrote to me to say that they had received the amended report,. . . but, needless to say, no new job offers were mentioned.

**08/03, TX.** My story is I am a 10 yr Marine Veteran with children under the age of 11. After serving my country I opened the door to a career in IT technologies as an Application Developer. I have worked for [several U.S. companies], and 3 international manufacturing corporation. In 1993, my brother used my name to avoid [being] arrested for a traffic ticket, since he had warrants. He did this because he knew I was [out of the country] at the time. Well in 1999, I found out while applying for a position [in TX], that I had a felony conviction ... dated 1993 listed under my name which showed as an alias for my brother. Was not hard to prove that I was in military and out of country, but still had to get fingerprinted to clear the matter up for good or so I thought. Well after losing my job in Aug 02, I have went through the normal motions of applying for jobs which were plentyful in my field. As to date I have to not even received one call back. I recently found out through the last potential employer, a friends of mine, that I had 2 felony convictions and about 6 class b misdemeanors convictions on my record. After research of publicdata.com and DPS online Convictions db, I learned that all my brother's convictions, etc, were under my record, name, dob, etc. This time instead of being an alias for my brother I was the principle criminal and he was my alias, which pointed back to my record.

**02/04, CA.** 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](http://www.choicepoint.com) & [www.backgroundchecks.com](http://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 Misdemeamor charge in Arizona.(same name & birthdate 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 to tell the next company that I submit my resume/cover letter & application to, that I am NOT that [Mr. X], who plead guilty in case number [xx] in Municipal Court in Glendale, AZ on [xx date]?

**02/04, TX.** In early February of this year I applied for a nighttime position with Company Q. I was called in for a nighttime interview by the HR Manager BB on 02/02/2003, who pulled my resume from an employee site. I met with a 3rd shift supervisor named MH who then asked that I be brought for a second interview with the Manager of the store and with BB. I was then offered

a position; I filled out the necessary paperwork and took a drug test. I did not hear back from BB and decided to call back on Friday and was informed that he was not in. On Saturday Morning BB contacted me and informed me that I was not going to be employed by Q because I lied that I had no felony convictions. I asked BB to repeat what he had stated and he said that he was looking at my consumer report and I have a DWI conviction and several pending warrants! He then informed me that I would be receiving the documentation to substantiate Q's choice not to hire me. I received the documentation via US Postal mail that afternoon and to my surprise the information contained was not for me but for another individual who had the same name but different birthdate as me! It is clear that the individual listed is not me but because [he] did not do his job accurately he figured I was just another Hispanic man with a felony conviction record who lied on his job application! The actual report even states: "While the information furnished is from reliable sources, its accuracy is not guaranteed. Proper use of this report and final verification of the named individual's identity is your sole responsibility." I have contacted Choice Point Services at their Atlanta location and I have reported an inaccuracy in my credit report. They have informed me that within 10 business days they will be researching and getting back to Q and myself regarding this grave error. I want to ensure that I have taken the proper steps so far and if I need to report this to the local authorities? I have since been offered another job but I am afraid that if the same information comes up they will think I am this individual on my credit report!

**01/04, NV.** I was terminated from CC due to the fact my background check was incorrect. It reflected a conviction in 1994 of petty theft and a charge involving minor children. The conviction was reduced to a fine for trespassing but the California system was not updated therefore to my employer it appeared as if I was a thief and irresponsible because children were involved. Needless to say the original incident occurred in 1994 and resolved in 1998. I wasn't even aware when I paid the fine it was considered a conviction. I thought once I paid it the situation was resolved and over with. The employer stated I intentionally lied on my application and there was no way I can prove I made an honest mistake. Not only this issue was at hand when I was terminated I was told to let this issue be a lesson to me and my family by the Human Resources director.

**01/04, no location.** ChoicePoint reports that I have felony arrests when in fact I haven't been arrested. Can the ChoicePoint report be corrected? It's impossible to find a job with felony arrest/convictions showing up. I wrote to ChoicePoint but never received word from them. This has been going on for approximately 5 years.

**01/04, CA.** I was convicted of a misdemeanor crime, but it was dismissed through PC 1203.4 [California statute that grants courts discretion, on certain conditions, to set aside a guilty verdict and dismiss charges]. I applied and received an offer from Company P, but after a background search was conducted, P 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 with a corrected consumer report, which stated that I had no convictions. However, P 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 P. But now that P denied the offer, I do not

have a job.

**11/03, NV.** After being denied employment or fired [from] several hotels here in las vegas, I obtained a copy of my "Police Scope" from the police. To my amazement there was a charge AND conviction of "battery with deadly weapon on a 65 year old person" I have been told by "paris" hotel in las vegas that this is sick & that I would be a liability to the company & put other employees in danger. This all stems from the "bogus" police reports that were obtained. I NEVER was arrested, went to court, or anything involving such a crime yet it REMAINS on my police report making it impossible for me to gain good employment here in Las Vegas.

**01/04, CA.** I was denied employment recently because of erroneous information in an employment background check. And there after begin requested to sign two separate forms for a more extensive background investigation from a third party entity, the company froze on its obligation to supply me a copy of the report, pursuant to my request to their attorney and directly to the company. The company, willfully refused to comply with the laws in this matter in California. The attorney actually acknowledges the existence of the reports and offers to provide a copy if his client will let him and I provide a release of further action against the company and his firm. I refused to provide them a release of anything. I continue to demand that they provide me with all the documentation associated with this pre-employment process in accordance with the written disclosures on the forms they provided and with the laws of this state.

**06/04, CA.** I applied for a retail position with a high-end women's clothier in San Francisco. I received a copy of a background check from a company called USMA. They list erroneous misdemeanors and felonies. How do I best clear this defamatory information?

**02/04, GA.** I have been a victim of Identity theft for quite sometime now. I have been to several law enforcement agencies and when I go to try to dispute the issue, it seems as if I am the suspect. What would be my first step at trying to resolve this issue. I have been to and contacted different law enforcement agencies and police departments and they have an actual photo of this person. They won't even give me documents to support this issue. The problem first came to my attention years ago when I couldn't get a job, and a decent place to live. I have contacted in person, The DD Police Dept., CP Police Dept., CL County police Dept., BB Police Dept. These are all in DD. Now I have been arrested on a misdemeanor case but never charged and I am thinking this is why they never will give me documents, but that has nothing to do with all these other charges that are on my criminal record

**Conclusion:** The above instances are just a few of the stories reported to the PRC. There are many other cases of workers harmed by inadequate privacy, lack of procedural protections, and inaccuracy in public record files and data vendor files. These stories all illustrate the distressing hall-of-mirrors effect that erroneous background checks can cause people who have information that is inaccurate or that does not belong to them incorporated into their records.

Such errors raise serious questions for employers and individuals alike. Who is this person? What is the truth? How does someone prove he is not the same person identified as a criminal in a commercial background check? The stories also illustrate the absolute necessity of a viable,

accessible redress process; and if a job is in the balance, redress must be completed before employment is denied or terminated.

Problems caused by misidentification and inaccurate or incomplete information can ruin the lives of innocent people. Without question, problems will occur with increasing frequency as background checks become even more common than they now are. In addition, the long string of security breaches and massive exposures of personal information reported since the ChoicePoint incident in February 2005<sup>16</sup> should serve as a warning that an unknown amount of that stolen or exposed data could be misused in ways that will further corrupt the accuracy of commercial databases.

For these reasons alone, before any move is made to include private employers and commercial data vendors, the Department should extensively study and report on the major issues of data accuracy and security. One recommendation is for the DOJ to conduct a study for accuracy by ordering background checks for a sample of 50 to 100 of its own employees and having the employees tabulate the errors they find in their own reports. The Department may divide the sampling among the private data vendors being considered as a supplement to IAFIS.

The Department should not permit private use of the federal data files, for either private employers or data vendors, unless the public can be confident that individual privacy will be strictly respected; that the subjects of reports receive full due process and effective redress; and that the accuracy and completeness of information furnished can be verified.

In closing, we appreciate the opportunity to share our views and experiences with the Department as it undertakes recommendations of highest importance to job applicants and employees.

Sincerely,



Beth Givens, Director  
Tena Friery, Research Director  
**Privacy Rights Clearinghouse**  
3100 5<sup>th</sup> Ave., Suite B  
San Diego, CA 92103  
(619) 298-3396  
[www.privacyrights.org](http://www.privacyrights.org)

Linda Ackerman  
Staff Counsel  
**Privacy Activism**  
San Francisco, CA  
[www.privacyactivism.org](http://www.privacyactivism.org)

---

<sup>16</sup> See “A Chronology of Data Breaches Reported Since the ChoicePoint Incident,” on the Privacy Rights Clearinghouse web site at <http://www.privacyrights.org/ar/ChronDataBreaches.htm> .