When your criminal past isn't yours

December 16 2011, By JORDAN ROBERTSON , AP Technology Writer

In this Dec. 18, 2010 photo, Kathleen Casey poses on a street in Cambridge, Mass. A case of mistaken identity landed Casey on the streets without a job or a home. The company hired to run her background check for a potential employer mistakenly found the wrong Kathleen Casey, who lived nearby but was 18 years younger and had a criminal record. (AP Photo/Michael Dwyer)

(AP) -- A clerical error landed Kathleen Casey on the streets.

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

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

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

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

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

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

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

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

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

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

Those are the results of an investigation by The Associated Press that included a review of thousands of pages of court filings and interviews

with dozens of court officials, data providers, lawyers, victims and regulators.

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

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

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

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

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

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

In some instances, their automated formulas misinterpret the

information provided them. Other times, as Casey discovered, records wind up assigned to the wrong people with a common name.

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

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

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

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

But those data do not always tell the full story.

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

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

Haynes relented and paid after six months. Anyone looking at Haynes'

physical file at the courthouse in Montgomery County, Pa., would have seen that the fraud charge had been removed. But it was still listed in the limited information on the court's website.

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

"I want my life back," Haynes says.

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

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

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

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

2004 to 2010. Individual payments will range from $15 to $20,000.

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

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

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

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

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

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

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

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

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

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

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

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

CoreLogic says its accuracy standards meet the law, and it seemed to

blame North Carolina, saying that the state's actions "directly contributed to the conditions which resulted in the alleged contract violations," but it would not elaborate. CourtTrax did not respond to requests for comment.

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

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

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

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

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

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

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

Data providers defend their accuracy. LexisNexis does more than 12

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

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

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

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

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

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

The industry says it polices itself and believes the approach is working.

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

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

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

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

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

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

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

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

One of Teague's lawyers, Jeff Myer of Legal Action of Wisconsin, an

advocacy law firm for poorer clients, says the state is protecting the sale of its lucrative databases.

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

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

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

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

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

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

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

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

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

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

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