★ **Roll Call Number**

Agenda Item Number 63

Date April 23, 2007

RESOLUTION APPROVING: i2 CONTRACT FOR LAW ENFORCEMENT INTELLIGENCE DATABASE

WHEREAS, this matter was brought before the City Council on the April 9, 2007 Roll Call No. 07-665, Council Communication No. 07-201; and,

WHEREAS, the City Council postponed this item to the April 23, 2007 Council Meeting in order that further information could be obtained for Council review; and,

WHEREAS, the City of Des Moines, Iowa Police Department is using a number of unsupported and disparate databases and large numbers of paper files to collect and store criminal intelligence information; and,

WHEREAS, the City of Des Moines, Iowa Police Department has no capability to incorporate open source information, or to query against the totality of the information, or to share the information horizontally across public safety agencies and those in the private sector with a need to know, or vertically among local, regional, state or federal agencies; and,

WHEREAS, the City of Des Moines, Iowa Police Department has a continuing need to exchange information and interact with Iowa Department of Public Safety's Intelligence Bureau, Fusion Center Hub and Law Enforcement Intelligence Network (LEIN), Iowa Department of Corrections, Midwest High Intensity Drug Trafficking Area (HIDTA) and the Mid-states Organized Crime Information Center (MOCIC) on a real time basis; and,

WHEREAS, the entities and agencies identified use i2's products for the entry and submission of criminal intelligence information, security, inquiry, dissemination, and review-and-purge processes in accordance with Federal Code of Regulations (28 CFR Part 23) *"Criminal Intelligence Systems Operating Policies"* and Iowa Code Chapter 692 *"Criminal History and Intelligence Data"*; and,

WHEREAS, the City of Des Moines entered into; Agreements with Iowa Homeland Security and Emergency Management Division for administration of Law Enforcement Terrorism Prevention Program funds to support the operation of the Region 5 Fusion Center and Intergovernmental 28E Agreements with Metropolitan Advisory Council (MAC) member communities for funding and implementation of Homeland Security Services; and,

WHEREAS, Municipal Code section 2-726 (a)(7) provides for a non-competitive procurement of goods and/or services that are of such a nature that they are the only goods and/or services which will fit and comply with the required use, or are an integral part of a total system so as to be uniquely compatible with existing city need, materials or equipment to be cost effective; and

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Des Moines, Iowa, that the i2 Contract, dated March 26, 2007 for software program licensing, implementation services and maintenance is hereby approved and the Mayor of the City of Des Moines, Iowa is hereby authorized and directed to sign said Contract and the City Clerk is hereby authorized and directed to attest to the Mayor's signature and the Chief of Police is directed to carry out the terms and conditions of the Contract and to purchase the computer hardware and operating system required to develop and operate the law enforcement intelligence database.

★ **Roll Call Number**

.....

Agenda Item Number
63

Date April 23, 2007

(Council Letter Number 07-244 attached)

Moved by _____ to adopt.

APPROVED AS TO FORM:

Doug Philiph
Assistant City Attorney

COUNCIL ACTION	YEAS	NAYS	PASS	ABSENT
COWNIE				
COLEMAN				
HENSLEY				
KIERNAN				
MAHAFFEY				
MEYER				
VLASSIS				
TOTAL				

MOTION CARRIED APPROVED

_____ Mayor

CERTIFICATE

I, DIANE RAUH, City Clerk of said City hereby certify that at a meeting of the City Council of said City of Des Moines, held on the above date, among other proceedings the above was adopted.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my seal the day and year first above written.

_____ City Clerk

63

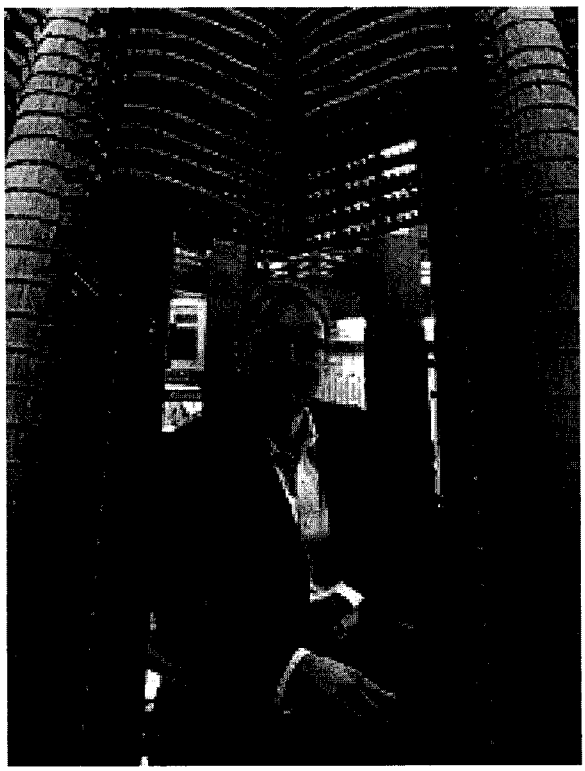
http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?_r=1&ref=technology&oref=slogin

Keeping Your Enemies Close

The New York Times

By Gary Rivlin, November 12, 2006

Alpharetta, Ga.



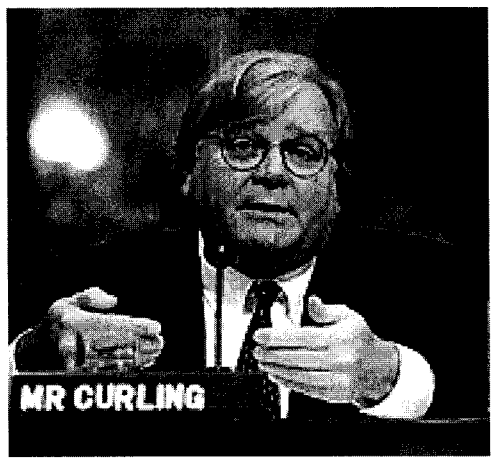
Darryl Lemecha, chief information officer at ChoicePoint, helps track client accounts for suspicious activity.

IF you found yourself running a company suddenly branded one of the most reviled in the country — if, for example, you noticed that visitors to Consumerist.com, a heavily visited consumer Web site, voted yours as the second "worst company in America" and you had just been awarded the 2005 "Lifetime Menace Award" by the human rights group Privacy International — you might feel obliged to take extraordinary steps. You might even want to reach out to your most vocal critics and ask them, "What are we doing wrong?"

So it was in early 2005 that Douglas C. Curling, the president of ChoicePoint, a giant data broker that maintains digital dossiers on nearly every adult in the United States, courted two critics whom he had accused just months earlier of starting "yet another inaccurate, misdirected and misleading attack" on his company.

Mr. Curling also contacted others who had spent years calling for laws requiring better safeguarding of personal information that ChoicePoint and other data brokers assemble — records such as Social Security numbers, birth dates, driver's license numbers, license plate numbers, spouse names, maiden names, addresses, criminal records, civil judgments and the purchase price of every parcel of property a person has ever owned.

"It was sort of like when I talk with my wife when she's not happy with me," Mr. Curling said of his dealings with some of ChoicePoint's harshest critics. "It's not exactly a dialogue I look forward to, but I can't deny it's important." He also could not deny his motivations for engaging in these conversations: in the public's mind, ChoicePoint



Douglas C. Curling, ChoicePoint president, on Capitol Hill in May 2005. He said a dialogue with critics was not pleasant but important.

had come to symbolize the cavalier manner in which corporations handled confidential data about consumers.

In January, the Federal Trade Commission hit ChoicePoint with a $10 million fine, the largest civil penalty in the agency's history, for security and record-handling procedures that violated the rights of consumers. Under the settlement, it also required ChoicePoint to set aside an additional $5 million to help those suffering financial harm because of its failure to provide adequate safeguards against data breaches.

But the financial penalties were nothing compared to the rehabilitation project confronting this hitherto invisible player in the global marketplace.

For years, ChoicePoint's top management had assured the world that it carefully protected its databases from intruders: Our systems are bulletproof. Intruder-proof. Believe us.

But then, in February 2005, the company had to acknowledge that it had focused so intently on preventing hackers from gaining access to its computers through digital back doors that it had simply overlooked real-world con artists strolling unnoticed through the front door.

Ultimately, ChoicePoint found that in 2005 alone, more than 40 phony businesses — thieves masquerading as bill collectors, private investigators, insurance agents and the like — had opened accounts that gave them unfettered, round-the-clock access to the vital data ChoicePoint maintains.

And, suddenly, the same privacy advocates that ChoicePoint had generally cast as shrill and ill-informed — a group that those inside the F.T.C. sometimes refer to as the "privacy posse" — proved crucial to its plans to both shore up its security and tend to its tattered image.

"I have to give them a lot of credit," said Daniel J. Solove, a posse member in good standing who had long been counted as one of ChoicePoint's most persistent critics. Mr. Solove, an associate professor at the George Washington University Law School, is among those whom ChoicePoint contacted shortly after its public relations debacle crested. "ChoicePoint had the attitude: 'We want to make our privacy practices exemplary,' " Mr. Solove said. "They wanted to find out what kinds of things they could do better and get feedback about some of the ideas they were thinking about."

For ChoicePoint, said James Lee, the company's chief marketing officer, the entire episode has proved an important learning experience. "The reality is, we were never as evil as people thought we were," Mr. Lee said, "but we were never as good as we thought we were."

Inside ChoicePoint, situated in a leafy office park in this suburb north of Atlanta, employees whistle with wonder over the talents of the various con artists — or "fraudsters," as company executives tend to call them — who finessed their way into their systems. According to the company, the fraudsters were wise enough to secure business licenses, thereby lending them a patina of legitimacy. They knew precisely what to write on their applications to convince ChoicePoint that their credentials made them fit for access to its databases.

"These guys were more sophisticated than anyone thought," Mr. Lee said, echoing the sentiment of many inside the company.

But the F.T.C. seemed to reach the opposite conclusion in a 33-page report it released earlier this year, after it completed an investigation of ChoicePoint. The commission found that ChoicePoint ignored "obvious red flags" because the company "did not have reasonable procedures to screen prospective subscribers." The report cast ChoicePoint's criminal

interlopers as sloppy and amateurish — but ultimately successful because their prey, a major company in the business of handling sensitive information, was alarmingly lax in its protection of its data repositories.

Signs that it was amateur hour inside ChoicePoint abounded, according to the F.T.C. report. The fraudsters faxed applications to ChoicePoint from a neighborhood Kinko's, listed post office boxes as primary business addresses and offered cellphone numbers as sole telephone contacts — which no one at ChoicePoint ever bothered to call anyway to establish the numbers' legitimacy. In at least one case, an approved applicant failed even to provide a last name, the F.T.C. found.

As ChoicePoint executives say, the fraudsters sometimes took the trouble to register their businesses with the state — but those documents should have set off alarms rather than justify the granting of an account.

The F.T.C. found that ChoicePoint accepted articles of incorporation that had been suspended or had expired, and "tax registration materials that showed that the business' registration was canceled." Then there were the contradictory addresses in the submitted documents — discrepancies that ChoicePoint employees accepted "without conducting further inquiry to resolve the contradiction," according to the commission's report.

"It was a well-known fact back then that ChoicePoint would do business pretty much with anyone who came along," said Robert Douglas, an information security consultant and editor of PrivacyToday who has done consulting work for ChoicePoint for several years. "They were making all the right noises about security but there wasn't any follow-through to back up their words."

Inside ChoicePoint, they like to say that the company is in the business of helping customers make informed decisions about whom they can trust.

Insurance companies and banks use its databases to help them decide who is a good credit risk and who is not. ChoicePoint sells its services to employers screening new hires, to landlords running background checks on new tenants, and to the 7,000 law-enforcement agencies and governments worldwide that the company counts as clients. Other customers include bill collectors, private investigators and media outlets, including The New York Times.

Yet a company with the snappy motto — "smarter decisions, safer world" — failed to use its resources to assess and then protect itself from some of its own customers. In some cases, the F.T.C. found, individuals were granted accounts "notwithstanding the fact that ChoicePoint's own internal reports on the applicant linked him or her to possible fraud." The company continued to furnish consumer reports to customers, the commission said, "even after receiving subpoenas from law enforcement authorities between 2001 and 2005 alerting it to fraudulent accounts."

Finally, in September 2004, ChoicePoint began to recognize that it had a major problem on its hands, when an employee in the company's new-accounts office realized that someone in the Los Angeles area, a Nigerian, was trying to set up multiple accounts, each time in the name of a different business.

The employee recognized the Nigerian's voice and alerted the company's security department, which in turn notified the local police. Although weeks would pass before senior executives learned of the troubling transactions with the Nigerian, the unfolding scam — and others like it — opened the eyes of outsiders to dangerous security lapses inside the company.

"I can assure you that now we learn immediately about this kind of problem," said ChoicePoint's chief executive, Derick V. Smith.

CHOICEPOINT was created in 1997 when Equifax, one of the big three credit reporting agencies — the others are TransUnion and Experian — spun off one of its divisions. Back then, the unit that would become ChoicePoint was involved in the labor-intensive and barely profitable business of maintaining claims histories on behalf of insurance companies. It also administered physicals, drug tests and the like for clients. Mr. Smith and Mr. Curling, who together ran what was then called the Insurance Services Group, foresaw a promising market in peddling data about individuals to a wider group of customers, and they convinced higher-ups that their unit should venture off on its own.

Since then, ChoicePoint has acquired more than 70 smaller companies and bought whatever databases it could get its hands on, including motor-vehicle reports from counties around the country, police records, property records, birth and death certificates, marriage and divorce decrees and criminal and civil court filings. These records had long been publicly available, but automation and superfast computers meant that comprehensive data dossiers could be assembled in seconds.

"It used to be that a business would have to go to 10 or 20 different vendors to get the same information that ChoicePoint sells in a single report," said Chris Jay Hoofnagle, a senior researcher at the Boalt Hall School of Law at the University of California, Berkeley, and a privacy advocate.

That approach has certainly proved lucrative. The company's stock price has quadrupled in nine years, and its revenue has, too, topping $1 billion in 2005. That growth has come despite stiff competition from two other companies of similar size that market background information about ordinary Americans: Acxiom, a publicly traded company based in Little Rock, Ark., and the LexisNexis Group, a division of Reed Elsevier. Many smaller companies are also in the business.

ChoicePoint sees itself as playing an essential, if not noble, role in the information economy. It has — at a reduced rate — helped nonprofits working with children identify registered sex offenders who applied for jobs, and it has provided the data that allowed the police to track down hundreds of missing children. Mr. Curling and others inside ChoicePoint argue that if there were no data brokers, home loans would take that much longer to secure and insurance rates would be based not on a person's driving record but on broad demographic categories, such as age and gender. Sure, breaches have been a problem, but theirs is still a young industry, ChoicePoint executives say.

"It takes time to establish best practices," Mr. Smith said.

It also took a state law. The data thieves who conned their way into ChoicePoint's system downloaded information about at least 166,000 individuals. In years past, the company would alert law enforcement officials when it suffered a data breach, according to Mr. Lee, and leave it at that. But under a California disclosure law passed in 2003, the company was required to notify every Californian whose personal details might have fallen into criminal hands.

"No one knows for sure, and no one can say, how many breaches occurred before California," Mr. Hoofnagle said. "This is an 'known unknown,' as Donald Rumsfeld would say."

RATHER than send letters only to the 42,000 Californians whose records had been downloaded by the fraudsters, ChoicePoint mailed a notice to all affected consumers, telling them that their

personal information might have fallen into the hands of identity thieves. Critics chided ChoicePoint for waiting about five weeks to contact consumers, but the company said it first needed to set up and staff a call center to handle the anticipated deluge of complaints.

"We knew that in all likelihood the first time that they were ever going to hear of ChoicePoint was in this letter," Mr. Lee said.

That would hardly be the last they would hear of ChoicePoint, however. Over the coming months, a long list of corporations and governmental agencies took their turn in the spotlight after they were obliged to acknowledge fumbling people's personal data: LexisNexis, Bank of America, Time Warner, Boeing, the Department of Veterans Affairs. And with each new breach, media accounts invariably mentioned the company whose breach had spurred a great awakening about the vulnerability of every individual's personal data — even if that company, ChoicePoint, had nothing to do with the other companies' woes.

Privacy critics were initially dubious when ChoicePoint contacted them in the wake of its February 2005 announcement. "Most gave us the Heisman," said Mr. Lee, who held out his forearm like a running back pushing away a would-be tackler to demonstrate his point. Yet, over time, most though not all of the privacy posse would agree to meet with Mr. Curling and other ChoicePoint executives, and walk away impressed by what they heard and saw.

That would include Professor Solove at George Washington ("They've implemented quite a number of measures to protect privacy"), Chris Hoofnagle at Berkeley ("ChoicePoint now has model security practices") and Beth Givens, director of the Privacy Rights Clearinghouse, a consumer advocacy group based in San Diego ("They've put in place practices that I wish all the data brokers would adopt").

Senator Charles E. Schumer, Democrat of New York, became an honorary member of the privacy posse when he declared the F.T.C. overly lenient for levying only a $10 million fine against ChoicePoint. But he, too, has changed his tune.

"I was worried that a fine would be seen as the cost of doing business," Mr. Schumer said in an interview. "But I have to say, ChoicePoint has become a model company."

Even Marc Rotenberg, a privacy posse member who refused to meet privately with Mr. Curling or anyone from ChoicePoint out of concern that doing so would undermine his credibility, begrudgingly gave ChoicePoint some praise.

"While I'm prepared to give them credit for a series of positive steps, I don't think it would be accurate to say that they got to this position on their own," said Mr. Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy rights group in Washington. "It took a lot of work by EPIC and other organizations."

When ChoicePoint started its makeover campaign, it first offered to rain down freebies on possible victims of identity theft, a protocol that others would follow. It invited them to join a credit monitoring service at no charge for one year, and provided them with free reports from the big three credit bureaus. To actual victims of identity theft, it offered its expertise to help correct the problem.

The company also gave a $1 million, four-year grant to the Identity Theft Resource Center, a nonprofit group in San Diego.

ChoicePoint then overhauled its security measures, a move that began with the hiring of Carol A. DiBattiste, who ultimately would fill the new position of chief privacy officer. Ms. DiBattiste is a

no-nonsense lawyer whose résumé includes 20 years in the Air Force and turns as an assistant United States attorney. To send the message that both security and privacy were a priority, Ms. DiBattiste was named the company's general counsel one year into her tenure Over the years, ChoicePoint had done a modest but lucrative business working with private investigators and other smaller enterprises. Shortly after its February 2005 announcement, the company said that it would no longer provide full Social Security numbers, birth dates or other sensitive information to these customers — data that Ms. DiBattiste called "keys to the castle."

That decision, Mr. Curling said, cost the company $15 million to $20 million last year. But inside ChoicePoint, executives saw that this small sliver of business threatened its overall reputation.

Until 2005, ChoicePoint had left credentialing to people in individual business units. It now has a centralized credentialing department. "The salespeople play no role in credentialing anymore," said Ms. DiBattiste, who deployed dozens of people to take on the painstaking chore of recredentialing every client that was not either a law-enforcement agency or a public company. ChoicePoint had 120,000 accounts before February 2005; it now has 104,000.

It also performs random audits of its customers, to ensure that they are conducting searches appropriate for their type of business, and it uses its computer systems to monitor accounts for suspicious activity.

"We look for any anomalies," said Darryl Lemecha, the company's chief information officer. "So if we see a 50-person company that typically does a background check like once a month suddenly do 20 in one day, we lock down that account so we can investigate."

ChoicePoint has endured roughly 100 outside audits, most of them conducted by long-term corporate customers, "and we passed them all," Ms. DiBattiste said. As part of its settlement, ChoicePoint agreed to submit to an F.T.C. audit every other year for the next 20 years.

It is not yet clear how many people were actually harmed by ChoicePoint's negligence. ChoicePoint says it knows of only 46 people who have been defrauded because of its data breach. But law enforcement officials have identified at least 800 people who have been identity theft victims because of ChoicePoint's missteps, said Betsy Broder, an assistant director at the privacy and identity protection unit of the F.T.C. But, she said, that number could rise.

"If data was stolen," Ms. Broder said, "nothing prevents the thieves from holding on to it for a period of time and using it perhaps when consumers let down their guard, or when the alert on their credit expires."

ChoicePoint also set up a Web site for consumers who, at no cost, want to check and challenge possible inaccuracies in their dossiers (www.choicetrust.com). "It's hard to overstate the significance of this,"

Ms. Givens said. "This is an important step forward in moving us to transparency."

Whether other companies follow suit remains to be seen. Michael Dores, founder of Merlin Information Services, a ChoicePoint competitor based in Kalispell, Mont., said he would offer free consumer reviews of its dossiers — but the cost, he said, "would put me out of business."

STILL, Mr. Dores said, ChoicePoint's own woes have had a big impact on Merlin, whose customers tend to be smaller businesspeople like debt collectors and private investigators. Like ChoicePoint, Merlin was fooled into providing an account to a fraudster.

So the company has recredentialed all its customers, Mr. Dores said, and created a new two-person compliance department. He said that Merlin now gives detailed personal data only to a small fraction of those to whom it provided such sensitive information in the past, much to the chagrin of many longtime customers.

Mr. Dores said he felt that he had no choice but to put these changes into effect, because "the Federal Trade Commission is in a bad mood over this stuff."

Members of the privacy posse still have their complaints about ChoicePoint.

Roughly 60 percent of its business falls under the Fair Credit Reporting Act, which regulates the collection and use of consumer credit information.

But to Mr. Hoofnagle and other privacy advocates, that is not enough. "If I had a magic wand I would make all of ChoicePoint's data fall under the Fair Credit Reporting Act," Mr. Hoofnagle said.

Even so, those who previously reserved most of their criticisms for ChoicePoint now aim their harshest words at some of its competitors. The same private investigators and others who formerly obtained Social Security numbers from ChoicePoint and Merlin are now simply seeking the services of other data brokers — companies such as Tracers Information Specialists of Spring Hills, Fla.

Yet Terry Kilburn, the chief operating officer of Tracers, said he was not worried about the hazards of providing such sensitive information. "We weren't the ones who were breached," Mr. Kilburn said. "Our security and compliance are strong, and so we are choosing to continue to do business the way we always have."

In Washington, legislators have proposed more than 20 bills to monitor data brokers more closely. According to Senator Schumer, ChoicePoint — in contrast to other large data brokers — has supported legislation he has proposed that would establish stricter security standards for any entity handling sensitive personal information.

"ChoicePoint, to its credit, got right behind our legislation and lobbied for it," Senator Schumer said. But the bill, which he and Senator Bill Nelson, Democrat of Florida, introduced in April 2005, has not passed, he said, "because a lot of other companies, quietly and behind the scenes, killed it."

Who's guarding your data in the cybervault?

USA TODAY, Monday, April 2, 2007

In a remarkable turnaround, ChoicePoint, the giant data broker excoriated two years ago for its lack of precautions as it went about gathering and selling personal data, has recast itself as a model corporate citizen.

California's milestone data-theft disclosure law forced ChoicePoint in February 2005 to reveal that it had sold sensitive information for at least 166,000 people to a Nigerian con artist posing as a debt collector. The Federal Trade Commission hit ChoicePoint with a record $10 million fine and ordered it to set aside $5 million to aid data breach victims.

The once-obscure data broker, tucked away in a nondescript business park 20 miles north of Atlanta, also embraced extensive reforms. The result: ChoicePoint is regarded by a dozen leading privacy advocates interviewed by USA TODAY as the most responsible company among dozens in the lightly regulated, fast-growing field of aggregating and selling sensitive information.

"ChoicePoint transformed itself from a poster child of data breaches to a role model for data security and privacy practices," says Gartner analyst Avivah Litan.

Despite ChoicePoint's makeover, there's rising concern among privacy experts and legislators about the frenetic business of assembling and distributing personal data. Everyone, it seems, wants Social Security numbers, birth dates, maiden names, criminal records, civil judgments and real estate records. Lenders, landlords and employers want as much data as they can get their hands on to size up applicants; law enforcement officials want it to track down criminals and terrorists. And cybercriminals are boosting demand for personal information as they concoct new Internet-enabled scams.

Data brokers such as ChoicePoint and LexisNexis assemble names, addresses, property records and other public records for use by everyone from employers to law enforcement agencies.

The Big Three credit-reporting agencies — Equifax,Experianand TransUnion — have a narrower focus. They compile data about car loans, credit card debt, mortgages and more to determine credit scores for lending institutions.

With a patchwork of state laws on data handling in place — and most data brokers just beginning to take basic precautions — the average citizen increasingly faces a new kind of multi-tiered jeopardy, law enforcement officials and privacy advocates say. Identity thieves often muck up data dossiers, while data brokers have little incentive to emphasize security or accuracy.

"You and I as consumers don't even know where all this information comes from or how it gets corrupted, and we have no way to fix it," says Mari Frank, an attorney and privacy consultant. "You can be denied credit or a job; you can be totally defamed; and you have no way to access the data to fix it — that's what's scary about the lack of privacy in the information age."

Scrutiny

Since its notorious data breach became public, ChoicePoint has imposed dozens of enhanced security policies. It has beefed up credentialing and auditing of customers and expanded an online service (www.choicetrust.com <http://www.choicetrust.com/servlet/com.kx.cs.servlets.CsServlet?usertype=c>) that lets individuals view their own records and make corrections for free. To underscore its Fort Knox-like approach, 26 surveillance screens form a backdrop at a guard's station at the main entrance.

All told, the company, whose annual revenue quadrupled over the past decade and now tops $1 billion a year, spent about $14 million tightening operations. It also exited the highly profitable business of selling Social Security numbers, birth dates and driver's license numbers to private detectives, mom-and-pop collections agencies and other small-time clients, giving up $15 million in annual revenue.

In a pivotal move, it recruited longtime Defense and Justice department official Carol DiBattiste to fill the new position of chief privacy officer and take over as general counsel at an annual compensation of about $800,000. That's more than twice what her peers earn, says Ari Schwartz, a privacy advocate and deputy director of Center for Democracy and Technology.

DiBattiste has steered the company through more than 80 audits by government agencies and big corporate clients to review its security and privacy procedures. "Arguably we were the most audited company in 2005 and 2006," says the energetic DiBattiste.

Privacy advocates worry that self-policing isn't enough; only a portion of what data brokers do falls under the federal Fair Credit Reporting Act, which regulates how the Big Three collect and disseminate consumer credit histories.

Data brokers argue that much of what they disseminate is not covered by federal rules "because it is based on public records" such as birth and death certificates, and property records, says Evan Hendricks, editor of Privacy Times newsletter.

Chris Hoofnagle, senior fellow to the Berkley Center for Law and Technology at the University of California-Berkeley, contends modern-data storage and data-mining technology has allowed data brokers to pervert the intent of open records law. "The government compels individuals to reveal their personal information in

a variety of contexts, then pours it into the public record for anyone to use," he says. Data brokers "collect the information, repackage it and return it back to the government and businesses full circle."

A bad dream

Critics such as Pam Dixon, executive director of World Privacy Forum, rail against the data brokers' practice of selling vast quantities of personal data to government agencies. ChoicePoint says less than 4% of revenue comes from the sale of data to government customers, but it won't name them.

Accuracy of data flowing to employers and creditors is a big concern. Dixon says if consumers had access to all of the data ChoicePoint supplies to the government, that "would be a tremendous help in easing the harms stemming from data inaccuracies." Erroneous profile data disrupt people's lives every day, privacy experts say.

James Derrell White, 41, who happens to live in Alpharetta, Ga., where ChoicePoint is based, was denied a job with Home Depot this year because data provided by ChoicePoint incorrectly identified him as a felon. "We thought we were in a bad dream," says Julie White, James' wife.

The data broker intermingled data for White and a felon with the same name and birth date. After the office of U.S. Rep. Tom Price, R-Ga., contacted ChoicePoint on the Whites' behalf, the matter was resolved and White got the job. ChoicePoint says it was already resolving the matter.

(Last week, ChoicePoint started a pilot program to give job applicants the chance to view their criminal background report at the same time as their potential employer.)

ChoicePoint says that its core mission is to help companies and government agencies temper risks.

Company executives, including chief marketing officer James Lee, have taken to repeating a catch phrase about ChoicePoint's earnestness dealing with critics: "It's like facing your wife when she's angry; it's not fun, but you learn something."

Deluge of breaches

By attempting to take the high road in the freewheeling data-brokering trade, ChoicePoint has spotlighted how an unregulated industry can police itself, Hoofnagle and others say.

DiBattiste says she has heard rumblings that other companies think "we're 'doing too much.' "

ChoicePoint's initiatives have had the effect of deflecting criminals' attention to less-attentive data brokers, as well as to all organizations storing large caches of personal information, Dixon says.

More than 500 incidents ranging from TJX to the Department of Veterans Affairs have been reported, involving records lost for tens of millions individuals since 2005. Privacy Rights Clearinghouse started the Chronology of Data Breaches list after ChoicePoint went public with its breach in February 2005.

A flurry of breaches reported last December — UCLA, 800,000 records stolen; Aetna, 130,000; and Boeing, 382,000 — pushed the number of records that have turned up missing over the 100 million mark; it recently topped 150 million. Yet Daniel Solove, an associate professor at the George Washington University Law School, and other privacy experts say Acxiom and LexisNexis "act as if nothing happened."

Executives at Acxiom and LexisNexis rebut such criticism. "Everything ChoicePoint has done since 2005, we already offer," says Jennifer Barrett, chief privacy officer at Acxiom, which specializes in lifestyle data — information about the reading and voting habits of consumers culled from public records and consumer surveys. LexisNexis spokeswoman Sue D'Agostino said the company is "confident that our security procedures are as robust as others in the industry."

Extending the market

Newer data brokers, such as ZabaSearch <http://zabasearch.com/> , Intelius, PrivateEye.com <http://www.privateeye.com/processor.asp?piid=46> and Voompeople.com <http://www.voompeople.com/processor.asp> , have stepped up efforts to extend the market for profiles to everyday consumers. PrivateEye.com, Voompeople.com and ZabaSearch did not respond to interview requests.

These online services typically require payment by credit card for background checks of varying thoroughness. Intelius is a representative example: It supplies data you can get on yourself — or anyone else — simply by typing a first and last name. This will usually pull down your home address and age, along with similar data on relatives who share your surname, as well as strangers with similar names.

Intelius' core business: enticing consumers to run $50 background checks on nannies, coaches, health care workers and the like.

Given transitory modern culture and the wide array of public records, inaccuracies are unavoidable, data brokers say. Inconveniences are offset by

peace of mind gained from verifying credentials, says Ed Petersen, Intelius vice president of sales and marketing.

Yet, more widely dispersed data also means more opportunity for criminals; identity thieves can secure sensitive data from the online brokers as easily as any consumer — and pay with stolen credit card numbers, says Idan Aharoni, senior fraud analyst at RSA, the security division of EMC.

Gartner estimates 15 million Americans will become victims of identity theft this year, up 50% from two years ago. "Since a fake ID is an integral part of most fraud operations, there are entire sections within the underground dedicated to forging IDs," Aharoni says.

Federal lawmakers, meanwhile, have begun to weigh in with proposed legislation.

Sens. Patrick Leahy, D-Vt., and Arlen Specter, R-Pa., would mandate consumers' rights to correct misinformation about them and allow federal agencies to assess the quality of data supplied by data brokers.

Sen. Dianne Feinstein, D-Calif., is seeking to ban the sale or display of people's Social Security numbers without their consent.

"No matter how good any company's attitudes toward privacy, there are too many players in the (data-collecting) industry — too many intricate parts when it comes to privacy issues — to expect self-regulation to effectively deal with the problems," Solove says.

Swartz reported from Alpharetta, Ga., Acohido from Seattle.