Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement

Chris Jay Hoofnagle [FNA1]

Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement, 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004)

I. Introduction

Traditionally, law enforcement officers obtained information by speaking with suspects' neighbors, employers, or friends. They would analyze paper arrest records and crime reports. In order to obtain personal information stored in private databases, they would have to call a variety of different vendors.

The shift to a digital environment has brought many changes to law enforcement's collection of information. Now, by visiting a single website, such as www.cpgov.com, law enforcement can obtain a comprehensive dossier on almost any adult. That website was custom-tailored for law enforcement by ChoicePoint, Inc. (ChoicePoint), a commercial data broker (CDB).

CDBs make available a wide variety of information, from arrest and court records to notice that a suspect has opened a private mailbox. Access to private sector databases has significantly altered the balance of power between law enforcement and the individual. As one internal document from the United States Marshals Service (USMS) put it:

With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, social security number), all known addresses, drivers license information, vehicle information ... telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc. fn1

This new power has been made possible by the confluence of fast network connections, the availability of public records, both electronic and paper, that are rich with personal information, fn2 and the alacrity of companies that have become very profitable from selling personal data to the government.

A number of risks to due process and privacy are raised by the collection and maintenance of information. The information could be used for political or personal purposes. Examples of police misuse of databases abound in the media, with violations found involving street-level local police officers to Federal Bureau of Investigation (FBI) and Drug Enforcement Administration (DEA) officers. There is also a general risk that the collection of information on individuals will upset the balance between government and individuals, resulting in a shift of power that is oppressive. In a report mandated by the Privacy Act of 1974, fn3 the Privacy Protection Study Commission highlighted this risk:

In a larger context, Americans must also be concerned about the long-term effect record-keeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset. fn4

There is nothing inherently wrong with law enforcement buying access to CDBs. After all, the private sector provides law enforcement with many tools, including pistols and batons. But there are strict rules for the use of these police tools. There is training to help ensure that pistols are only fired with justification, and that batons are employed properly. If these tools are misused, there are serious repercussions, including the discipline or dismissal of the officer and section 1983 lawsuits. fn5 The Electronic Privacy Information Center (EPIC) is exploring whether similar substantive and procedural safeguards are in place for law enforcement officers who use CDBs to gain access to personal information. Specifically, EPIC is evaluating what, if any, safeguards are in place to protect individuals' privacy and due process rights.

To answer these questions, in June 2001, EPIC filed a series of requests under the Freedom of Information Act (FOIA) fn6 seeking access to government records regarding companies that sell personal information to the

government. Almost three years and a lawsuit later, EPIC has obtained over 1,500 pages of material from nine agencies about ChoicePoint and other CDBs. In this article, findings are presented from the requests, and concerns are raised regarding law enforcement access to personal information. The conclusion sets forth a framework of privacy protections to address risks to due process and the Fourth Amendment posed by companies like ChoicePoint. Based on the findings, the Privacy Act of 1974 should be extended to CDBs, as they regularly serve as private escrows for information that the government could not otherwise collect legally. Furthermore, there should be broader protections for personal information in public records, as these sources form perhaps the greatest threat to the future of data privacy.

Determining agency practices from FOIA documents is difficult. There are few "smoking gun" FOIA documents. Rather, analysis requires viewing many different documents in context to determine agency action. Because of these limitations, documents are interpreted conservatively, and I have indicated in the text where there are ambiguities in the documents.

The analysis is also limited by the willingness of agencies to provide documents. Of the agencies covered by EPIC's request, the USMS released the largest number of unredacted documents. The FBI, on the other hand, had the greatest number of documents responsive to the FOIA request, but the substantial majority of this material was either heavily redacted or withheld in full. As a result, practices of certain agencies receive more analysis than others.

This article begins, in Part II, with a description of the information found in the FOIA requests. In Part III, it applies American privacy law to the use of CDBs. It concludes, in Part IV, with several recommendations for policymakers, including extension of the Privacy Act to CDBs that sell information to government and the need to reevaluate public records policy in the United States.

II. Findings from the FOIA Requests

On June 22, 2001, EPIC filed FOIA requests with seven agencies seeking access to records "concerning businesses that sell individuals' personal information." fn7 Several agencies initially rejected the request, arguing that EPIC needed to further specify the topic for the search of records. In those cases, EPIC specified that the request sought all records related to ChoicePoint, LexisNexis, Experian, Dun & Bradstreet, and Database Technologies Online.

In January 2002, EPIC filed suit in the United States District Court for the District of Columbia against all seven agencies for failure to comply with the FOIA's requirements. fn8 That litigation is still pending. EPIC continues to seek 5,000 pages of ChoicePoint contracting documents held by the FBI's Criminal Investigative Division. EPIC also seeks access to a Department of Justice (DOJ) memorandum from the agency's Office of Professional Responsibility. That document concerns an internal investigation regarding unauthorized disclosure of agency information. The issues are fully briefed and are awaiting a ruling from the court.

Since filing the requests, EPIC has received over 1,500 documents. fn9 The documents led to six major findings. First, the documents show that law enforcement can quickly obtain a broad array of personal information about individuals. Second, although EPIC filed a broad request for documents, there was almost no evidence of controls to prevent agency employees from misusing the databases. It appears as though auditing employee use of the databases is either impossible or simply not done. Third, the database companies are extremely solicitous to the government and actually design the databases for law enforcement use. Fourth, ChoicePoint expanded significantly in 2000 by starting to acquire and sell personal information of non-citizens. That discovery has led to strong international dissent. Fifth, many of the contracts with CDBs are sole-sourced, meaning the contracts are not open to competitive bidding. Sixth, the FBI has a secret, sole-source contract with ChoicePoint to develop an information service prototype.

A. Scope of Information Available to Law Enforcement

"One stop mind-boggling power." fn10

Federal law enforcement agencies have access to a broad array of personal data on both citizens and non-citizens. One document obtained from the USMS describes the agency's requirement that CDBs "produce a comprehensive profile on an individual, generated by only one or two queries." fn11 This power has resulted in considerable benefit to the agencies. fn12 And the agency uses it extensively; agency documents claim that the USMS ran 20,000 searches per month in the late 1990s. fn13 Actual invoices dating from February 1999 to September 2001 show that the agency ran between 14,000 and 40,000 searches per month. fn14 A document from the FBI's Public Source Information Program claims that the use of CDBs has increased by 9,600% since 1992. fn15

1. ChoicePoint, Inc.

ChoicePoint, Inc. is a company based in Alpharetta, Georgia, that concentrates on selling information and data services to insurers, businesses, government, and direct marketers. fn16 Last year alone, ChoicePoint amassed revenues of over $ 795,700,000. fn17

ChoicePoint has managed to attain a large share of the CDB market with strategic purchases of other businesses. fn18 In 2000, ChoicePoint purchased DBT Online, Inc., a successful CDB that provides "AutotrackXP," a favored law enforcement-oriented service. fn19 In 2001, it purchased the Osborn Group, Inc., and in 2002, it purchased Vital Chek Network, Inc. and Vital Chek Network of Canada, Inc., the largest suppliers of vital records (birth, death, marriage, and divorce certificates) in the United States and Canada. fn20

ChoicePoint owns a number of other subsidiaries in Texas, Delaware, Kansas, Arizona, Illinois, Tennessee, and Pennsylvania. fn21 These subsidiaries include EquiSearch Services, Inc. (asset recovery), Insurity, Inc. (insurance software), National Data Retrieval, Inc. (public records collection), Resident Data Financial, LLC (data collection), Resident Data, Inc. (data collection), and The Bode Technology Group, Inc. (forensic DNA and offender databanking). fn22

ChoicePoint sells a wide array of information to the government, including: fn23

. Credit headers, a list of identifying information that appears at the top of a credit report. This information includes name, spouse's name, address, previous address, phone number, Social Security number, and employer;

. "Workplace Solutions Pre-Employment Screening," which includes financial reports, education verification, reference verification, felony check, motor vehicle record, SSN verification, and professional credential verification; fn24

. Asset Location Services; fn25

. The ability to engage in "wild card searches," which allows law enforcement to "obtain a comprehensive personal profile in a matter of minutes" with only a first name or partial address; fn26

. The use of "Soundex" queries, which allow searches on personal information based on how names sound, rather than how they are spelled; fn27 and

. Information on neighbors and family members of a suspect; fn28

ChoicePoint's AutoTrackXP is one of the most favored CDB products. fn29 It provides an interface for additional data points, including: fn30

. Linkage services, which draw graphical relationships between suspects and other addresses, neighbors, and Social Security Numbers;

. Public records, including Social Security Death Master Filings, bookings and arrests, liens, judgments, and bankruptcies;

. Licenses, including drivers, pilots, and professional credentials;

. Lists of residents of Georgia, New York, and Ohio; fn31

. National, real-time phone directories and reverse look-up services; fn32

. Business information, compiled nationwide from Secretaries of State; fn33

. "SmartSeach," a tool that allows broad wildcard searches: "There may be thousands of Jane Does, but there's probably only one Jane Doe who's between 25 and 30 and lives on the upper west side of Manhattan. SmartSearch makes it possible to find that one"; fn34

. U.S. Military Personnel; and

. Boat owners;

ChoicePoint also offered an "Interactive Pager Service" in 2000 to the USMS. fn35 Under the arrangement, Marshals would receive two-way pagers that delivered ChoicePoint reports wirelessly. fn36

2. LexisNexis

LexisNexis, a corporation owned by the United Kingdom-based Reed Elsevier, offers access to numerous databases and information retrieval services. fn37 Through services such as its featured search tool, "SmartLinx," LexisNexis offers access to Social Security Numbers, addresses, licenses, real estate holdings, bankruptcies, liens, marital status, and other personal information. fn38 It bills itself as the market leader in the United Kingdom and the British Commonwealth and as a major publisher in Continental Europe and Latin America. fn39

LexisNexis began in Dayton, Ohio as a contractor for data and information to the U.S. Air Force. fn40 In 1979, the company began to offer news and business information, and in 1987, the company purchased Michie, which, at the time, was the sole provider of statutes for thirty-five U.S. states and territories. fn41 In 1997, LexisNexis debuted the first web-based service for U.S. legal professionals. fn42 In 2003, LexisNexis merged with Canada's Quicklaw, Inc. to form LexisNexis Canada. fn43

Reed Elsevier additionally acquired the legal publishing Butterworths Group in 1970, which had operations in India, Canada, Australia, New Zealand, and South Africa. fn44 It acquired Martindale-Hubbell, publisher of the renowned law directory, in 1990. fn45 Since 1998, Reed Elsevier has acquired U.S. legal publisher Matthew Bender and leading citator Shepard's Company. fn46

LexisNexis provides services to the USMS, including the "location of witnesses, suspects, informants, criminals, parolees in criminal investigations, location of witnesses, parties in civil actions." fn47 LexisNexis' Person Tracker Plus Social Security Number is a private library "designed to meet the needs of law enforcement." fn48 It provides information probably derived from credit headers, including the name, social security number, current address, two prior addresses, aliases, birth date, and telephone number on an individual. fn49 The company also provides the P-FIND white pages directory; information on pilots, military personnel, and professional licenses; driver's licenses for Florida, Massachusetts, Texas, and Wisconsin; and access to the Social Security death master file. fn50

3. Dun & Bradstreet

Dun & Bradstreet (D&B) is a provider of credit, marketing, purchasing information, and commercial receivables, with offices in over forty countries. fn51 Last year alone, D&B amassed revenues of over $ 1.38 billion globally. fn52

D&B was founded as the Mercantile Agency in New York City in 1841, as the world's first business information provider. fn53 The current D&B Corporation was formed upon the separation of Moody's Corporation on September 30, 2000. fn54 At the end of last year, D&B had over sixty subsidiaries worldwide. fn55

D&B is growing rapidly. For example, during 2002, the Global D&B database grew by over 10 million records, to cover a total of 80 million businesses; over 40,000 new family tree members were added to the database, bringing the total number of globally linked businesses to 7.6 million. fn56 Nearly 372,000 new businesses from the Asia Pacific region were added to the D&B database. fn57 In addition, approximately 390,000 new businesses from the Latin America region were added to the D&B database. fn58 Finally, the U.S. Marketing file increased by over 3 million records, to cover nearly 18 million businesses. fn59

Companies highly value D&B assessments of their businesses. It is unclear, however, if the executives at the companies understand that D&B eagerly sells reports not only to investors, but also to the government. In marketing materials obtained from the government, the company writes that D&B:

Maintains the largest commercial databases of business information in the world, including information on the largest Fortune 500 companies [unreadable] mom & pops who are doing business from their home. In fact, 85% of our records have less than 20 employees, and 97% of these records contain ownership details. fn60

The company's marketing materials list four full pages of data elements available to the government, including assets, the age of the executives, credit information, socio-economic indicators, and the telecommunications capability of the company. fn61

4. Experian, Inc.

Experian, Inc., a CDB based in Nottingham, United Kingdom and Costa Mesa, California, is a subsidiary of GUS pic, a U.K.-based holding company that includes retail, property investment, finance, and information services businesses. fn62 Experian offers a wide range of information and database services, including the sale of credit reports and credit headers. fn63 The information included in such credit reports includes the availability of credit, bankruptcy information, newly opened trades, the presence of a mortgage, recent credit inquiries, delinquencies, judgments, and liens. fn64

Experian also runs an extensive direct marketing business, selling consumer financial, educational, racial, and family information. fn65 Experian maintains records on approximately 215 million U.S. consumers fn66 and more than 15 million U.S. businesses. fn67 The company's medical databases include lists of individuals suffering from incontinence, prostate problems, and clinical depression. fn68

The Internal Revenue Service (IRS) uses Experian to obtain credit reports. fn69

B. Lack of Protections Against Insider Abuse

"Sed quis custodiet ipsos custodes?" fn70

Juvenal made this statement to ridicule Roman men who attempted to control the sexual fidelity of their wives by providing them with male guards. fn71 Juvenal's mocking statement has gained gravitas over the centuries, and it is now a serious question posed to those trusted with power: How does one supervise the authorities and ensure that government power is exercised with responsibility?

Supervising the authorities is a difficult task because literally tens of thousands of federal law enforcement agents have access to CDBs. fn72 A memorandum from the IRS shows that after the agency purchased services from ChoicePoint and Experian, it initially issued usernames and passwords to over 12,000 employees. fn73 The same document indicated that "additional end user names will be transmitted to ChoicePoint in the future." fn74 With the personal information of so many people at the fingertips of thousands of government agents, agencies need to establish sound measures to ensure responsibility.

One way to watch the watchers is to regularly audit access to CDB files. By doing so, a supervising officer can track personal use or other misuse of CDBs. Simple procedures, such as requiring an officer to keep an access log and to record the purpose for which searches are performed, can help promote a culture of accountability with personal information. However, these common sense precautions do not appear to have been implemented at any agency. fn75

Since the agency's query records are held at the CDB, normally the CDB could audit or track suspicious behavior. But for good reasons, auditing at the CDB is technically impossible. The agencies have arranged for "cloaked" access. This type of access "prevents anybody inside or outside the Company from tracking records a law enforcement user is researching." fn76 Without cloaked access, employees of the CDB could monitor law enforcement investigations and possibly tip off suspects. Requirements for cloaking may have been adopted after it came to light that Edward Asher, the founder of DBT Online (who later founded Seisint, the principal company behind the Multistate Anti-Terrorism Information Exchange, or "MATRIX"), was suspected of having ties to drug smugglers. fn77 News of this impropriety caused the DEA to suspend access to the company's main law enforcement product, AutoTrack. fn78

If access to the CDB is cloaked, auditing would have to occur at the government agency. But no document obtained from the government discusses auditing of law enforcement access as a regular policy to ensure honesty. In fact, the documents suggest that no auditing to prevent employee misuse occurs at all. This inference comes from a heavily redacted memorandum, where the DOJ Office of Professional Responsibility reviewed "Misconduct Allegations [redacted] Concerning Unauthorized Disclosure of Information." fn79 At one point in the investigation, a government employee uses ChoicePoint to search for personal information: "According to [redacted] conducted a "Choicepoint data search' and discovered recent credit activity [redacted] was alive [redacted]." fn80 In the "Discussion" section of the same memo, the text of a footnote suggests that auditing is not required and does not occur:

[redacted] requested a review [redacted] to determine the existence of any record of a Choicepoint database search. FBI [redacted] advised DOJ OPR that "no such record was found," but further stated that no such record is required to be maintained. FBI [redacted] also asked Choicepoint to conduct a review of its internal records to determine whether [redacted] performed a credit check of [redacted]. A representative of Choicepoint advised the FBI that the security parameters of its database do not permit Choicepoint to make such an inquiry. fn81

The latter portion of that paragraph refers to the "cloaking" that prevents ChoicePoint from viewing government queries of the database. fn82 It is reasonable to conclude that the first portion refers to the government's attempt to determine employee use of the database, and it appears that the government did not have, nor did it require, an audit trail. fn83

Other agency documents discuss information security, but in most cases, the measures are in place to protect the agency, rather than the privacy of individuals. For instance, one document from the USMS specifies that there are access restrictions for use of CDBs: "We must ensure that these [access lines to the database] are only being used for authorized purposes." fn84 But it becomes clear that the agency is primarily concerned about Marshals running searches for colleagues in other agencies, a technical violation of the contract with the CDB: "Any unauthorized purpose, such as running queries for another law enforcement agency, may prevent someone in another district from running queries for a USMS investigation." fn85

In crafting access restrictions, the USMS is also concerned about the traffic load on the computers. Too many searches could exclude other branches or offices from running searches: "We also ask that queries be run as quickly as possible during peak hours and be mindful of other users nationwide. The extensive "browsing' type searches should be saved for early or late hours in the workday, or after hours." fn86

Another agency memorandum does warn that use of CDBs for "non-law enforcement purposes is prohibited." fn87 But merely prohibiting the behavior is unlikely to deter individuals from misusing the CDBs. If the agency does not audit, individuals can misuse the CDB and face only a small risk of detection.

C. Data is Tailored to Government

The sale of personal information goes far beyond simply making the data available to government. ChoicePoint and others tailor their data for law enforcement agencies. A sales pitch from DBT Online, a company now owned by ChoicePoint, reads in part: "AutoTrack Plus was designed with law enforcement in mind. DBT created its services with

the help of law enforcement and continues to maintain sworn law enforcement officers on site." fn88 Indeed, in a 1998 letter to the USMS, a DBT Vice President congratulates the agency for buying a subscription to AutoTrack Plus:

During my tenure as Special Agent of the DEA's Florida Division I became aware of AutoTrack PLUS as an exciting, new and truly innovative investigative resource ... . I selected AutoTrack PLUS as the database resource for all of the DEA's offices in Florida. The system quickly became an integral part of our investigative process.

And after 26 years with the DEA, I retired and joined Database Technologies, Inc. as a Vice President. My goal here is to introduce AutoTrack PLUS to every member of the law enforcement community throughout our nation ... . To that end, every law enforcement agency is extended an automatic 33% discount on our service. fn89

DBT even circulated a special newsletter for law enforcement subscribers. fn90

ChoicePoint was highly rated by its agency clients. In a review of ChoicePoint's services performed by a USMS employee, the company earned a perfect score and a strong written accolade: "ChoicePoint is very responsive to the Marshals Services and has made enhancements to their public information database (CDB Infotek) to meet our needs." fn91

D. The International Dimension

In 2000, ChoicePoint began collecting international data. fn92 In marketing materials fn93 provided to the Immigration and Naturalization Service (INS), the company emphasized that the information was legally obtained from official sources in compliance with the Foreign Corrupt Practices Act (FCPA). fn94 The INS has obtained cloaked access to ChoicePoint databases for the agency's "Quick Response Teams" and "Headquarters Investigation Division." fn95 In 2001, the agency ran approximately 20,000 "domestic" searches monthly, and 3,000 international searches. fn96 Eighty to ninety percent of the international searches were on Mexican citizens. fn97

INS authorities chose ChoicePoint as their main CDB because it had a broad array of personal information on non-citizens. ChoicePoint is the only vendor capable of providing online access to the following data sets: complete listings of all Mexican, Colombian, and Argentine Citizens; inclusion of unlisted numbers in Mexico, Brazil, and Argentina; Mexican vehicle and driver license data; Colombian company data; and Brazilian business people. fn98

A ChoicePoint marketing paper describes the source of the information available more fully. It appears as though ChoicePoint is selling information from Mexico's voter registration rolls, a practice that is illegal in most American states. fn99 A Mexico citizen registry database has a nationwide listing of "all Mexican citizens registered to vote as of the 2000 national election ... . Data includes full name(s), legal addresses, [date of birth], Place of Birth, Gender and identification information." fn100

For Columbia, ChoicePoint planned to offer a national registry file of all adults, "including date and place of birth, gender, parentage, physical description, marital status, registration date, registration and passport number, and registered profession." fn101 Similar databases exist for Argentina and Costa Rica. fn102

In April 2002, EPIC obtained and posted documents showing this extensive information sale by ChoicePoint. On April 14, 2003, Jim Krane of the Associated Press wrote an article about the sale of this information that ran in newspapers internationally. fn103 Public reaction to this news was intense. ChoicePoint quickly issued statements to sooth the situation, claiming that the data was legally acquired from third-party vendors. fn104 But whether the data was obtained legally did not matter to the individuals whose information was sold. fn105 The sale was morally objectionable to them, and threatened the integrity of their elections process and the very sovereignty of their countries. fn106 Legal experts from the region disagreed with ChoicePoint's assessment. One legal expert described the sale as "espionage." fn107 Tec de Monterrey University Professor Julio Tellez argued that the information on Mexicans could only be used for elections, and its use for impermissible purposes subjected ChoicePoint and the U.S. government to suit. fn108

Within two days, the Presidents of Nicaragua and Costa Rica announced investigations into the sale, and Mexican officials hinted that the country would retaliate against the United States at an upcoming United Nations meeting. fn109

Later that week, Nicaraguan authorities raided businesses thought to have sold information to ChoicePoint. fn110 Mexican authorities eventually placed three suspects under house arrest; the charge was treason. fn111

The American government was monitoring these developments. Documents obtained from the American Embassy in San Jose show that the government was monitoring news reports covering the information transfer. fn112 On April 15, 2003, the American Embassy in Mexico sent a confidential action cable regarding the controversy to several agencies, including the DOJ, the Department of Homeland Security, the Department of Treasury, the Central Intelligence Agency, the White House, and the National Security Council. fn113 The message noted that the Mexican media had covered the sale of personal information from the federal elections institute database, and that officials had already filed a complaint against unnamed election officials. The Embassy noted that "a potential firestorm may be brewing" fn114 and that ChoicePoint's spokesperson had confirmed that American government "agencies regularly use ChoicePoint information for fighting drug trafficking and terrorism." fn115 The cable closes, "Most importantly, embassy requests guidance for press inquires." fn116

The embassies discussed generating public relations materials to shape the debate. In an e-mail from the American Embassy in Managua, a public relations officer asked colleagues to find "articles or writers on this issue." fn117 The public relations officer continued:

The kind of article I am thinking of would outline the debate within the U.S. about the extent of government access to electronic info and efforts to pass laws that restrict that access ... . The article shouldn't be one-sided and alarmist, but rather point to the difficult challenge of striking a balance, and to make clear that this is a dynamic process. If a good article like this exists, we might try and get rights. If the article doesn't exist, we might think about commissioning a writer. fn118

Eventually, the news of the sale sparked calls for privacy reform in Central and Latin America. The President of Costa Rica later proposed legislation that would limit the sale of databases containing personal information. fn119 In addition, five other countries reconsidered passing comprehensive database privacy legislation. fn120

It is worth asking why the reaction to ChoicePoint activities was so intense in other countries, while in the United States, less critical attention has been directed at these practices. It could be because Americans have already been inundated with the public relations strategies that the American Embassies discussed. It could be because Americans trust domestic companies and law enforcement; perhaps if Canada or some other country collected troves of information on Americans, the public would become upset.

In any case, ChoicePoint seems to be expanding its access to personal information of non-citizens: "ChoicePoint ... is actively seeking to add data from other countries in Latin America, Asia, and Europe." fn121 The company will face serious challenges in doing so, especially if other nations implement comprehensive data protection acts to prevent uncontrolled access and aggregation of personal information.

E. Sole-Source Contracts

Many of the contracts with ChoicePoint are "sole-sourced," that is, they are not open to competitive bidding. Since sole-source bidding may be unfair or wasteful, agencies must justify their decisions to avoid the competitive bidding process.

The agencies have heavily redacted documents that justify sole-sourcing. For instance, in seeking a sole-sourced contract for AutoTrackXP, all justifications for the lack of a competitive bidding process were fully withheld. fn122 The IRS withheld the "Statement of Need," "Trade-offs," "Risks," and even the "Product Descriptions." fn123 A July 1999 press release from DBT Online announced that AutoTrackXP is available on the General Services Administration award schedule. fn124 This allows an agency to purchase the service automatically, without entering into competitive bidding.

Several federal agencies buy access to ChoicePoint data through the DOJ's Justice Management Division. fn125 The DOJ maintains a "Telecommunications Services Staff" that facilitates the data sale. This arrangement allows smaller agencies to more quickly gain access to CDB services at a lower cost and without having to issue solicitations for contracts.

F. The FBI's Criminal Investigative Division Has a Secret, Sole-Sourced Contract with ChoicePoint

The FBI released documents that refer to a secret, classified contract between the agency's Criminal Investigative Division and ChoicePoint. fn126 The documents contain a discussion of the agency's justification for awarding a sole-source contract to ChoicePoint. The agency reasons that such an arrangement is necessary because revealing the topic of the contract to other companies would endanger national security. fn127 Specifically, it would expose the Criminal Investigative Division and National Security Division operations to risk. fn128 After learning of the release of these documents, the DOJ urgently requested the documents back from EPIC and another requester. fn129 The Department recently asked a court to fully exclude the classified contract from EPIC's FOIA request. fn130

The documents are heavily redacted, and the reader is invited to infer their meaning. One contract schedule describes the following service: "The Criminal Investigative Division (CID) [redacted] has a requirement to conduct a feasibility study for a prototype methodology to meet the requirements of the Federal Bureau of Investigation's (FBI), [redacted] Program." fn131 The term for this prototype methodology is nine months.

Both parties wished to keep the prototype under wraps. The contract has severe terms, specifying that if the agency releases proprietary information, it will constitute a material breach of the contract. fn132 Proprietary information was to be released to the FBI only on a need-to-know basis. Under one draft of the contract, if ChoicePoint released FBI law enforcement information, it also would constitute a material breach. One agency employee working on the contract wrote after this provision: "[CAN WE GET SOME LIFE OR DEATH LANGUAGE FOR HERE?]." fn133 ChoicePoint employees with access to the FBI facility housing the prototype had to have "secret" level security clearances. fn134

III. Role of Privacy Law is Unclear

American privacy law tends to be sectoral and context based. Unlike other nations, the United States lacks a comprehensive privacy law to protect data. Information is protected based on the sector of the economy regulated and sometimes the context in which the information is collected. For instance, medical information communicated to a health provider is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPPA). fn135 However, when a consumer completes a product warranty card that requests details about ailments, that information can be freely sold to anyone for any purpose. Similarly, cable companies face strict rules limiting the use of data on viewers' behaviors, but the law does not extend to intermediate devices, such as a Tivo personal video recorder. Tivo, Inc. can sell the same information that the cable company cannot. Privacy law in the United States is riddled with similar deficits in protection.

A 2001 FBI memorandum analyzed the application of privacy law to CDBs. The agency's Office of General Counsel considered whether ChoicePoint could be used for foreign intelligence and counterterrorism purposes. fn136 Much of the analysis is redacted, but the agency concludes that the use of ChoicePoint is consistent with privacy law and DOJ regulations:

In summary, it is our opinion that, as stated in the DOJ Online Guidelines, "obtaining information from online facilities configured for public access is a minimally intrusive law enforcement activity." In this regard, individuals "do not have a reasonable expectation of privacy in personal information that has been made publicly available ... ." Finally, the Attorney General Guidelines do not preclude the use of an Internet resource, such as ChoicePoint, to obtain publicly available identifying data concerning either known or unknown persons. fn137

In a routing slip that appears to accompany this memorandum, an FBI employee writes: "you may use ChoicePoint to your heart's content." fn138

James Dempsey and Lara Flint argued in 2003 that "an analysis of existing law shows that there are, in fact, few legal constraints on government access to commercial databases ... . Laws on specific categories of commercial data are riddled with exceptions for law enforcement or intelligence uses." fn139

While it is true that Congress and the courts have allowed the government broad access to personal information held by commercial organizations, privacy protections apply in some cases. It is apparent at least to the CDBs that privacy laws apply to some extent. Their contracts with agencies are peppered with requirements to comply with several privacy laws. CDBs view certain federal privacy laws as limiting their activities, but the scope of those limits is unclear. These limits are explored in the section below. The best prospect for meaningful privacy protection flows from the Fair Credit Reporting Act. fn140 Other acts have been interpreted narrowly, or were written to regulate specific sectors of the economy that do not reach CDBs.

A. The Fourth Amendment

The Fourth Amendment prohibits unreasonable searches and seizures. fn141 It has been up to courts to define the bounds of "unreasonable" and "search." In Katz v. United States, the Supreme Court adopted the modern test, one where the government is prohibited from intruding into zones where individuals enjoy a "reasonable expectation of privacy." fn142 Justice Harlan's concurring opinion set forth two requirements for a constitutionally-recognized zone of privacy: (1) it must be a place that a person subjectively believes to be private; and (2) society must be prepared to recognize the zone as private. fn143

The Supreme Court decided in United States v. Miller that individuals do not have a reasonable expectation of privacy in information provided to others. fn144 As a result, law enforcement agencies do not need a warrant or subpoena to obtain information from a large array of sources that hold personal data. Dempsey and Flint discuss some categories of sensitive information that can be acquired easily by law enforcement agencies as a result of Miller. Such information includes travel records, store purchases (from books to groceries), automated toll records, building access records, real estate information, utility bills, club memberships, and magazine subscriptions. fn145

News reports following the September 11, 2001 attacks indicated that law enforcement agencies increased requests to private parties for communications information. fn146 In particular, internet service providers (ISPs) were targeted by these requests. The Seattle Times quoted Al Gidari of Perkins Cole describing this increase: "What we've seen after Sept. 11 - at least in the United States - is about a fivefold increase in the number of subpoenas requested of service providers, and frankly ... just requests for information." fn147

Furthermore, some private businesses have crafted "law enforcement-friendly" policies that exploit the Miller case in order to provide data to government. In a closed-door conference in February 2003, eBay, the world's largest Internet auction site, revealed that it had crafted its privacy policy to maximize efficiency in responding to law enforcement requests for personal data. fn148 eBay described in detail how the company "is willing to hand over everything it knows about visitors to its web site that might be of interest to an investigator." fn149 eBay's Joseph Sullivan, director of the company's Law Enforcement and Compliance Department, specified that law enforcement only need to ask for the information they wish to obtain: "There's no need for a court order." fn150 The article specifies that law enforcement requests for data are sometimes delivered by e-mail or fax.

The shortsighted Miller decision does not take into account the reality that individuals need to give their information to third parties in order to participate in society. It is unfair to cede all individuals' rights to a company that can simply hand over personal information to law enforcement. Congress acted swiftly to reverse the Miller decision with respect to financial records, fn151 and several state supreme courts have rejected the Miller approach. fn152

The current conception of protections under the Fourth Amendment provides individuals with little protection against CDBs.

B. The Privacy Act

Some contracting documents fn153 require ChoicePoint to fully comply with the Privacy Act. fn154 The Privacy Act of 1974 requires government agencies to apply a full set of "Fair Information Practices" to systems of records that contain personal information. fn155 Principally, the Act prohibits amassing personal information unless the agency has a proper purpose for doing so. Once collected, personal information is subject to a series of rights. The government must give notice of all the databases it maintains. It must provide access and correction rights. It must limit collection to only the information necessary to fulfill a specified government function. Finally, data must be destroyed after a certain period of time.

The Act only applies to the federal government and to private companies that are administering a system of records for the government. fn156 When the information originates from the government and is transferred to a private company, Privacy Act requirements apply to the contractor. For instance, in a contract between ChoicePoint and the USMS, when the agency transfers fugitive data to the company, Privacy Act obligations accompany the data. fn157 However, a database of information that originates at a CDB would not trigger the requirements of the Privacy Act. In fact, credit reporting agencies are specifically exempted from being considered a federal contractor for systems of records. fn158

This limitation to the Privacy Act is critical - it allows CDBs to amass huge databases that the government is legally prohibited from creating. Then, when the government needs the information, it can request it from the CDB. At that

point, the personal information would be subject to the Privacy Act, but law enforcement and intelligence agencies have special exemptions under the Act that limit access, accuracy, and correction rights. fn159

C. The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) fn160 was the first federal law to regulate private-sector use and disclosure of personal information. It offers the greatest opportunities for protection of data held by CDBs. The law regulates the collection, maintenance, and dissemination of "credit reports." The law is opt-in; that is, individuals must consent to release of their credit reports unless the transfer of data is authorized under a specific section of the Act. fn161

Under the law, police have a number of avenues to access credit reports. Full credit reports can be accessed by court order, by grand jury subpoena, or by request of a child support enforcement agency. fn162 Credit information can be obtained through three other FCRA provisions. The Act allows the FBI access to individuals' account information and identifying information for counterintelligence purposes upon written request. fn163 A provision added by the USA PATRIOT Act fn164 allows any government agency with a counterintelligence purpose to obtain the full credit file upon written certification that it is necessary for either an investigation or intelligence analysis. fn165 Another section allows any government agency to obtain credit headers, identifying information from a credit report, upon request. fn166

The FBI has interpreted the FCRA artfully in order to evade all of the requirements and procedures of the Act. The FCRA has a poorly drafted definition of "consumer report" that has allowed some to narrow the Act's coverage in a way that contradicts Congress' intent. The Act conditions the definition of "credit report" on how the information is used. That is, a "credit report" is any communication bearing on a consumer's character or general reputation, which is used for credit evaluation, employment screening, insurance underwriting, or licensing. fn167 Some have used this awkward construction to limit the scope of the Act, resulting in absurd, unintended consequences. One could argue, for instance, that a criminal who obtains credit information from a bureau, but uses it for fraud, has not triggered the Act, because fraud is not one of the enumerated uses of a "credit report."

The FBI uses similar reasoning to evade protections of the FCRA: "In this instance, none of the information which the FBI would seek to review has been collected by ChoicePoint for any of the [FCRA] purposes." fn168 The agency further concludes that ChoicePoint is not a credit reporting agency: "Because ChoicePoint does not collect "public record information' for any of the highlighted purposes, ChoicePoint is not acting as a "consumer reporting agency' for the purposes of the FCRA and the collected information therefore does not constitute a "consumer report.'" fn169

Both of these conclusions are based on a strained reading of the Act which contravenes the intent of Congress. The provisions governing law enforcement access make it clear that Congress intended procedural safeguards against disclosure of credit information, regardless of its intended use.

Two courts have rejected the reasoning underlying the FBI's logic, although no court has ruled directly on the issue of whether law enforcement access to CDBs triggers the FCRA. As Dempsey and Flint note in their review of federal privacy law and access to commercial information, some courts have ruled that when information is collected for credit reporting purposes, it remains a credit report, despite the fact that it may be employed for non-FCRA purposes. fn170

There are FCRA-style contract requirements in an agreement to provide the USMS with interactive pagers that transmit ChoicePoint information wirelessly. fn171 The agreement places ChoicePoint under a burden to assure "maximum possible accuracy" of information reported to the agency, and requires the company to "reinvestigate" any information disputed by the agency. Both of these terms are taken from the FCRA.

D. The Gramm-Leach-Bliley Act

Some agency documents fn172 discuss compliance with the Gramm-Leach-Bliley Act (GLBA). fn173 That law allows individuals to opt-out of a limited amount of information sharing among financial services companies, including credit reporting agencies. fn174 The Act specifically allows disclosure of personal information to law enforcement agencies. fn175 It also preserves law enforcement access to financial records under the Right to Financial Privacy Act. fn176 Furthermore, the GLBA contains a savings clause that preserves the ability of law enforcement to obtain personal information under the standards of the FCRA summarized above. fn177

The GLBA requires financial services institutions to develop privacy and security safeguards for non-public personal information, but law enforcement agencies are not subject to this requirement. fn178 The only prohibition that

might apply to law enforcement is a requirement that information not be passed on to third parties or used for secondary purposes, such as direct marketing. fn179

E. Driver's Privacy Protection Act

Since 1998, the Driver's Privacy Protection Act (DPPA) fn180 has required state motor vehicle administrators to gain opt-in consent before selling personal information. fn181 The Act principally provides protection by preventing release of information from the state to CDBs. fn182 However, both ChoicePoint and LexisNexis offer to sell motor vehicle administration information on residents of Texas and Florida. fn183 At least three class action suits have been initiated against CDBs for these practices. fn184

The Act only protects information at motor vehicle administrations. Once information leaves the state administration office and is transferred to a CDB, the Act's protections do not apply. Furthermore, the Act does not protect information on the driver's license, thus allowing businesses to capture and sell data from identification cards. Some businesses regularly "swipe" licenses now, collecting all the information off the card, and resell it. fn185

F. The Self-Regulatory Individual Reference Services Group Principles

Some documents fn186 require the law enforcement agency to comply with the Individual Reference Services Group (IRSG) Principles. fn187 The IRSG was formed in order to manage fomenting criticism regarding companies that sold personal information. fn188 After passage of the GLBA in 1999, the group dissolved, but some members still adhere to the IRSG Principles. The Principles set forth a weak framework of protections, allowing companies to sell non-public personal information "without restriction" to "qualified subscribers," which include law enforcement agencies. fn189 So-called "qualified subscribers" need only state a valid purpose for obtaining the information and agree to limit redissemination of information. fn190 Under IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but ChoicePoint does not consider its customers to be members of the general public:

ChoicePoint limits access to its information products to government and businesses with legitimate business purposes for the data, such as detecting and preventing fraud, performing legal due diligence, locating criminal suspects, finding missing children, and managing business risks in a variety of ways. We feel that removing information from these products would render them less useful for important business purposes, many of which ultimately benefit consumers. ChoicePoint DOES NOT DISTRIBUTE NON-PUBLIC INFORMATION (as defined in the Principles) TO THE GENERAL PUBLIC PURSUANT TO SECTION V(C) OF THE PRINCIPLES. The general public therefore has NO direct access to or use of NON-PUBLIC INFORMATION (as defined in the Principles) from ChoicePoint whatsoever. fn191

The IRSG Principles have been carefully crafted in order to ensure maximum flexibility by CDBs. They have failed to set forth a reasonable degree of protection for individuals. Accordingly, recommended protections are suggested in the next section to promote privacy.

IV. Recommended Protections

Because collection of information empowers the state and private businesses over individuals, a system of protections is recommended for personal data. Law enforcement access to personal information databases is not inherently problematic. But there has to be reasonable limits on that access, unless we are comfortable in becoming a dossier society.

There should be four principal changes in public policy to better accommodate the rights of individuals in their data. First, government and businesses should minimize the amount of information collected on individuals. When these entities collect less information, it is difficult for CDBs to amass dossiers on individuals. Second, policymakers should no longer make distinctions between commercial and government collection of information. Policymakers often set different standards for information collection, reasoning that commercial actors pose less risk than government information collectors. This distinction is no longer tenable with the cozy relationships between CDBs and the government described in this article. Third, we must realign public records policy so that it is compatible with modern technology. The amount of personal information poured into public registers, combined with the absence of limits on use of the data, poses serious risks to privacy. Fourth, the Privacy Act of 1974 should apply to CDBs. These companies

are performing government functions and allowing the government to have access to dossiers that otherwise could not be assembled.

A. Minimization

The first principle in privacy protection is the practice of minimizing data collection. Minimization is the process of reducing the amount of personal information collected from individuals. Often, commercial transactions can be performed with no exchange of recorded personal information. We experience this every day by engaging in cash transactions. We even have anonymous authentication systems in the real world, such as subway passes and movie tickets, that give us access to services without leaving any identifying information. Minimizing information collection cuts off dossier-building at the source.

Some companies are voluntarily engaging in minimization as a result of post 9/11 incursions into civil liberties. Bear Pond Books in Montpelier, Vermont, for instance, is purging the consumer records of those who request it, and has erased records held by members of its readers' club. fn192

B. Drop Untenable Distinctions Between Government and Commercial Collectors

U.S. constitutional, common, and statutory law has long recognized that government access to personal information presents risks to individuals' privacy and autonomy. Our nation also has a deep suspicion of government action and motives, while maintaining trust in the action of the private sector.

Libertarians and conservatives have employed persuasive arguments to stave off privacy regulation that affects the commercial sector. They have argued that government collection, use, and disclosure of information presents more risk than commercial collection because the government has the power to arrest, imprison, and even to execute citizens. Commercial entities, although they hold our mortgages and often control our employment, arguably present less risk to our autonomy. But as this article shows, this distinction between the risks of government and commercial privacy risk is no longer tenable. Commercial actors provide personal information to the government in a number of contexts, and often with astonishing alacrity.

The illusory nature of the distinction becomes clear when one reviews the documents obtained from the government agencies. Some of the agencies have news clippings that track privacy limitations on the private sector, or on access to public records. fn193 These include news clippings on the right to opt-out under state laws from sharing Maryland motor vehicle information and the Supreme Court's upholding of the DPPA. Government agents understand that limits on the commercial sector will ultimately reduce their access to personal information. Indeed, one presentation from the FBI's Public Source Information Project noted that the passage of the GLBA coupled with litigation in the D.C. Circuit "limit[ed] access to Credit Header information." fn194 It further noted that the law has a law enforcement exception, but "at least one of the credit bureaus has stated that they will no longer make credit header information." fn195 An IRS memorandum notes that:

ChoicePoint will provide public record information ... . The coverage is national, but will vary based on the availability of data from specific states and counties. For example, ChoicePoint provides DMV data ... . However, due to California's Anti-Stalking laws, that state will not sell DMV information to any 3rd-party vendor, and thus no California DMV data will be available. fn196

In an unrelated FOIA request, EPIC obtained an e-mail fn197 from an employee at the Defense Advanced Research Projects Agency sent to Total Information Awareness developers John Poindexter and Robert Popp. fn198 The e-mail discusses private-sector CDB Acxiom as a supplier for Total Information Awareness' mega-databases of personal information:

Acxiom is the nation's largest commercial data warehouse company ($ 1B/year) with customers like Citibank, Walmart, and other companies whose names you know. They have a history of treating privacy issues fairly and they don't advertise at all. As a result they haven't been hurt as much as ChoicePoint, Seisint, etc. by privacy concerns and press inquiries. fn199

The e-mail claims that Jennifer Barrett, Acxiom's Chief Privacy Officer, gave recommendations that would help quell public scrutiny of the transfer of data from the company to the government:

One of the key suggestions she made is that people will object to Big Brother, wide-coverage databases, but they don't object to use of relevant data for specific purposes that we can all agree on. Rather than getting all the data for any purpose, we should start with the goal, tracking terrorists to avoid attacks, and then identify the data needed (although we can't define all of this, we can say that our templates and models of terrorists are good places to start). Already, this guidance has shaped my thinking. fn200

The employee continues: "Ultimately, the US [sic] may need huge databases of commercial transactions that cover the world or certain areas outside the US [sic]. This information provides economic utility, and thus provides two reasons why foreign countries would be interested. Acxiom could build this mega-scale database." fn201

In the 1990s, privacy advocates warned the public about the risks to privacy that were posed by Acxiom and other direct marketers. The worst case scenario painted by privacy advocates is contained in the DARPA e-mail described above: a situation where direct marketers and CDBs cooperated with law enforcement to create ultra-large databases of personal information. In response to this criticism, the Direct Marketing Association (DMA), which is the main industry group representing commercial collectors of information, touted its self-regulatory ethical guidelines. Article 32 of the guidelines specifies that "Marketing data should be used only for marketing purposes." fn202

In numerous representations to the media and regulators, DMA officials and direct marketers attempted to quell criticism surrounding the possibility of law enforcement access to marketing data. As early as 1993, DMA president Jonah Gitlitz attempted to avoid regulation by promising limited use of direct marketing information: "It's hard to say what the future of regulation will be, but our stance is that as long as (direct marketers) continue to use information for marketing purposes only, and use it responsibly, there should be no problem in the implementation of data in direct marketing for advertisers." fn203

In 1997, the DMA renewed this promise, stating in a filing to the Federal Trade Commission that:

The Direct Marketing Association has long had a policy opposing the use of personal data obtained from marketing transactions for non-marketing purposes. Our Guidelines therefore limit the sources of the information used by look-up services. Companies that maintain databases of both marketing and non-marketing information ensure that information gained from marketing transactions is not used as an information source for the look-up database.

The DMA's Guidelines for Personal Information Protection indicate that personal information collected for marketing "should only be used" for marketing purposes. This was the basis for The DMA's response to a December 20, 1994 Federal Register notice in which the Internal Revenue Service suggested that agency personnel would begin accessing commercial databases as part of its Compliance 2000 program. The DMA filed comments and led a public outcry against the proposal. DMA stated: "Commercial lists used by DMA members were created for the purposes of marketing and were never intended to be used for any other purpose." The IRS backed away from its intention to use marketing data for law enforcement.

In addition, The DMA Committee on Ethical Business Practice reviews complaints it occasionally receives regarding the alleged use of marketing data for non-marketing purposes. The Ethics Committee reviews these complaints to ensure that companies' use of marketing data is in accordance with the guidelines of The DMA. fn204

These promises worked. The federal government adopted a policy of self-regulation, allowing the continued collection of personal information in the private sector. These policies in turn led to our current situation where troves of personal information are available to both the government and the private sector.

If we are ever unfortunate enough to have George Orwell's Big Brother fn205 in the United States, it will be made possible by the private sector. It is time to drop distinctions between governmental and commercial collection of personal information. Both types of collection present the same risks, and it is foolish for us to continue to act otherwise.

C. Address Emerging Privacy Issues Presented by Personal Information in Public Records

"Like other vendors in the field, DBT acquires and "repackages' publicly-available data into its own formats and makes them available through its own query and reporting mechanisms." fn206

Much of the personal information made available to law enforcement originates from public records. In a variety of contexts, the government compels individuals to reveal their personal information, and then pours it into the public record for anyone to use for any purpose. fn207 The private sector has collected the information, repackaged it, and brought it back to the government full circle.

Privacy expert Robert Ellis Smith published a list of personal information that appears in court records systems in various states. fn208 The list includes medical records, Social Security numbers, victim's names, credit card and account numbers, psychiatric evaluation reports, juror's names, tax returns, payroll information, vehicle identification and driver's license numbers, and family profiles. fn209 It is unfair to have this information systematically poured into the public record and used for any purpose by the private sector.

If we wish to limit law enforcement power in this arena, we must find a policy for public records that reflects Twenty-first Century technology. Our current policy for public records was developed in a day where all information was on paper, dispersed across the country in small courthouses. Information was poorly indexed; periodically, it was destroyed by fire, improper storage, or negligence. Access was difficult enough. Aggregation was impossible.

Today vast quantities of personal information flow into the public domain from electronic court filings, arrest records, land sales, and dozens of other interactions that individuals have with the government. It is not enough, however, to focus only on electronic public records because the CDBs employ "stringers" to obtain information from paper records. ChoicePoint has a "staff of more than 1,500 researchers who obtain public record information from courthouses and other public sources on a daily basis." fn210

States that allow broad access to public records are supplying troves of data to law enforcement. For instance, ChoicePoint's AutoTrackXP services include thirty-six extra databases on Florida residents and seven extra on Texans. fn211 Access to information on Florida residents is particularly broad. It includes marriage records, beverage licensees, concealed weapons permits, day care licensees, handicapped parking permits, "sweepstakes," worker compensation, medical malpractice, and salt water product licensees. fn212

Public record policy in America was designed to protect people from government power; to provide a window into the operations of officials and thus a check on arbitrary or abusive exercise of authority. To a large extent, access to public records has served this purpose. But with electronic access and the power of aggregation, these policies have increasingly shifted to benefit the government and businesses. We need to realign these policies so that less personal information appears in the public record, while maintaining access to documents that allows for investigation and oversight of government.

D. The Privacy Act Should Apply to Private Sector Companies That Sell Information to the Government

The Privacy Act was enacted, in part, because of the specter of a federal data clearinghouse, one central place where all personal information could be stored for government access. fn213 When the law was passed in 1974, Congress envisioned that only the government could have the incentive and precious computing resources to build such a data clearinghouse.

Similarly, dystopian depictions of the future, including those made in George Orwell's 1984, fn214 saw government as the entity hungry for personal information of individuals. The reality is that arrays of individuals are interested in amassing individuals' personal information. As Professor Daniel Solove has argued, public policymakers should see information architecture as less Orwellian and more Kafkaesque; a dizzying array of private and public-sector actors have strong interests in tracking individuals and building dossiers of their personal information. fn215

In passing the Privacy Act, legislators added section m, which was included in order to prevent the government from simply farming out data operations in order to avoid the Act's responsibilities. fn216 Section m, as explained above, applies to systems of records created by a government, but administered by a private entity. It does not create rights or responsibilities in data collected by the private sector and delivered to the government at its request.

Subsection m falls short of the protections necessary to safeguard privacy. Companies in the business of collecting personal information for sale to the government should be held to Privacy Act responsibilities. It simply does not make

sense to maintain the current framework; one where the private sector has created the very federal data center that was so feared in the 1960s and 1970s. Our law should not allow an end-run around protections where the private sector can escrow troves of personal information custom-tailored for the government.

V. Conclusion

In passing the Privacy Act of 1974, Congress placed limits on the Executive branch's collection, maintenance, and use of personal information. But those protections have failed to meet Congress' intent because the private sector has done what the government has been prohibited from doing. Private sector commercial data brokers have built massive data centers with personal information custom-tailored to law enforcement agents. This has upset the balance of power between individuals and the government, allowing the police to peer into our lives from their desktops. Current privacy law does little to establish rights and responsibilities in the collection and maintenance of this information, in part because the government has employed artful interpretations of the Fair Credit Reporting Act to avoid privacy protections.

The release and use of public records containing personal information must be reevaluated, with three goals in mind. First, in order to promote privacy while accommodating legitimate law enforcement investigations, policymakers should establish a framework of rights that limit the collection of information. Second, they should cease to make policy distinctions between government and private sector collections of information. Third, the Privacy Act should apply to companies that regularly sell personal information to the government. Only after these protections are in place will "personal" information truly be personal.

[FNA1] Associate Director, Electronic Privacy Information Center (EPIC). EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. I wish to thank Woodrow Neal Hartzog, a candidate for LL.M. at The George Washington Law School, for his research and comment on this article.

fn1. Sole Source Justification for Autotrack (Database Technologies) (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02j.pdf [hereinafter Sole Source Justification for Autotrack (Database Technologies)].

fn2. Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1084 (2002); see Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 Minn. L. Rev. 1137, 1152-54 (2002) (explaining how the digitization of records has made personal information documents more accessible and less secure) [hereinafter Access and Aggregation].

fn3. See discussion infra Part III.B.

fn4. Privacy Prot. Study Comm'n, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission (1977), available at http://www.epic.org/privacy/ppsc1977report/c1.htm. [hereinafter Personal Privacy in an Information Society].

fn5. 42 U.S.C. 1983 (2000) (providing a civil remedy for citizens whose civil rights have been violated by government actors).

fn6. 5 U.S.C. 552 (2000).

fn7. The seven agencies were the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), the United States Marshals Service (USMS), the Internal Revenue Service (IRS), the Immigration and Naturalization Service (INS), and the Bureau of Alcohol, Tobacco and Firearms (ATF).

fn8. Elec. Privacy Info. Ctr. v. DOJ, No. 02-0063 (D.D.C. filed Jan. 14, 2002). The complaint in the case may be accessed online at http://www.epic.org/privacy/litigation/profilingcomplaint.html (last visited Mar. 27, 2004).

fn9. All of the documents are available online for review at EPIC's website, at http://epic.org/privacy/choicepoint.

fn10. AutoTrackXP, DBT Online News (DBT Online, Inc., Boca Raton, FL), Oct. 1999 (document obtained from the USMS), available at http://www.epic.org/privacy/choicepoint/cpusms7.30.02d.pdf [hereinafter AutoTrackXP].

fn11. CBD Notice for AutoTrack (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02b.pdf.

fn12. See FBI, The FBI's Public Source Information Program: Fact Versus Fiction (n.d.) (document obtained from the FBI) (reporting that in the Butte and Savannah areas alone in FY 2000, 524 arrests were made using public source information programs, and those areas only accounted for 4% of the FBI's total searches), available at http://epic.org/privacy/choicepoint/cpfbia.pdf [hereinafter Fact Versus Fiction].

fn13. Exhibit V-1: Customer Reference (n.d.) (document obtained from the USMS) available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn14. See ChoicePoint, Invoice Summaries (Feb. 28, 1999 to Sept. 30, 2001) (documents obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02h.pdf.

fn15. Fact Versus Fiction, supra note 12.

fn16. Electronic Privacy Information Center, ChoicePoint, at http://www.epic.org/privacy/choicepoint (last updated Feb. 14, 2004) [hereinafter ChoicePoint].

fn17. ChoicePoint, ChoicePoint Reports Fourth Quarter and 2003 Full Year Results (Jan. 22, 2004), at http://www.choicepoint.net/choicepoint/news.nsf/PR_FinEarn?OpenForm.

fn18. ChoicePoint, supra note 16.

fn19. Id.

fn20. Id.

fn21. Id.

fn22. Id.

fn23. Id.

fn24. ChoicePoint, Pricing Schedule C (Apr. 11, 2002) (document obtained from the DEA), available at http://epic.org/privacy/choicepoint/cpdea7.3.02.pdf.

fn25. Memorandum from David A. Mader, Assistant Deputy Commissioner Operations, IRS, to All Executives and Managers (Feb. 28, 2001) (document obtained from the IRS), available at http://www.epic.org/privacy/choicepoint/cpirs9.10.01a.pdf [hereinafter Memorandum to All Executives and Managers].

fn26. Sole Source Justification for Autotrack (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf; Soundex (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf.

fn27. USMS, CDB Notice for AutoTrack (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02b.pdf.

fn28. The Discovery Detail Report (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn29. ChoicePoint, supra note 16.

fn30. Id.

fn31. ChoicePoint, Pricing Schedule D (Apr. 11, 2002) (document obtained from the DEA), available at http://epic.org/privacy/choicepoint/cpdea7.3.02.pdf [hereinafter Pricing Schedule D].

fn32. Check Out What's New, Online With AutoTrack (DBT Online, Inc., Boca Raton, FL), Spring 1999 (document obtained from the USMS), available at http://www.epic.org/privacy/choicepoint/cpusms7.30.02d.pdf.

fn33. Id.

fn34. AutoTrackXP, supra note 10.

fn35. ChoicePoint, Interactive Pager Service Agreement (May 17, 2000) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf [hereinafter Interactive Pager Service Agreement].

fn36. Id.

fn37. LexisNexis, Company History, at http://www.lexis-nexis.com/presscenter/mediakit/history.asp (last visited Mar. 27, 2004) [hereinafter Company History].

fn38. LexisNexis, SmartLinx, at http://www.lexis-nexis.com/smartlinx/ (last visited Mar. 27, 2004).

fn39. LexisNexis, Company Description, at http://www.lexis-nexis.com/presscenter/mediakit/description.asp (last visited Mar. 27, 2004).

fn40. Company History, supra note 37.

fn41. Id.

fn42. Id.

fn43. Id.

fn44. Id.

fn45. Id.

fn46. Id.

fn47. LexisNexis, Exhibit B: Lexis-Nexis Select Limited Distribution Authorized Use List (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn48. LexisNexis, Fax Bulletin (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn49. Id.

fn50. Id. The Social Security death master file is a list of deceased person's Social Security numbers. Id.

fn51. See generally, Dun & Bradstreet, http://www.dnb.com (last visited Mar. 27, 2004) (providing a list of country offices and websites).

fn52. Dun & Bradstreet, D&B Announces 2003 Fourth Quarter and Full Year Results (Feb. 2, 2004), at http://www.dnb.com/US/about/index.html.

fn53. Dun & Bradstreet, The History of D&B, at http://www.dnb.com/us/about/company_story/dnbhistory.html (last visited Mar. 27, 2004) [hereinafter The History of D&B].

fn54. Id.

fn55. Dun & Bradstreet, Form 10-K for the Period December 31, 2003 (Mar. 5, 2004), at http://media.corporate-ir.net/media_files/nys/dnb/reports/2003_10K.pdf.

fn56. Dun & Bradstreet, Facts & Figures, at http://www.dnb.com/us/about/db_database/dnbstatistics.html (last visited Mar. 27, 2004).

fn57. Id.

fn58. Id.

fn59. Id.

fn60. E-mail from Jennifer Schaus, Dunn & Bradstreet, to Sharma Bahwana, Contract Specialist, INS (Sept. 27, 2001) (document obtained from the INS), available at http://epic.org/privacy/choicepoint/cpins3.25.02a.pdf.

fn61. Dun & Bradstreet, Data Elements Available from Dun & Bradstreet (Sept. 27, 2001) (document obtained from the INS), available at http://epic.org/privacy/choicepoint/cpins3.25.02a.pdf.

fn62. Experian, About Experian (2004), at http://www.experian.com/about.html.

fn63. See Experian, Company Profile (2004), at http://www.experian.com/corporate/index.html [hereinafter Company Profile].

fn64. See Experian, Sample Credit Report (2004), at http://www.experian.com/consumer_online_products/credit_manager.html#. The company delivered more than 2.7 million credit scores in 2003. Company Profile, supra note 63. Currently, more than 1.6 million members belong to its credit monitoring service. Id.

fn65. Chris Jay Hoofnagle, Barriers to the Constitutional Right to Privacy: Big Business Is Keeping an Eye On You, S.F. Chron., Jan. 29, 2004, at A23, available at http://sfgate.com/cgibin/article.cgi?file=/chronicle/archive/2004/01/29/EDGH14JBAFN1.DTL (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn66. Experian, INSOURCE (2004), at http://www.experian.com/products/insource.html.

fn67. Experian, Choose the Best Prospect Lists (2004), at http://www.experian.com/direct_marketing/acquire_customers/prospect_lists.html.

fn68. Hoofnagle, supra note 65.

fn69. Memorandum to All Executives and Managers, supra note 25.

fn70. Juvenal, Satire VI: Juvenal and Persius, ll. 346-7 (G. G. Ramsay trans., G.P. Putnam's Sons 1918) (translated, "But who is to guard the guards themselves?").

fn71. Id. ("I hear all this time the advice of my old friends - "Put on a lock and keep your wife indoors.' Yes, but who will ward the warders? The wife arranges accordingly and begins with them.").

fn72. See Memorandum to All Executives and Managers, supra note 25.

fn73. Id.

fn74. Id.

fn75. See IRS, Statement of Work: Section C (n.d.) (document obtained from the IRS), available at http://www.epic.org/privacy/choicepoint/cpirs9.10.01a.pdf. The IRS has session auditing, enabling the agent to recall all searches during one session use. Session auditing is inadequate to deter misuse of the CDB and the agency was emphatic in specifying that audits should be available only for one session. See id.

fn76. DBT's AutoTrackXP.com Secure, Anti-Fraud Web Site Listed on GSA Award Schedule, DBT Online News (DBT Online, Inc., Boca Raton, FL), July 8, 1999 (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf [hereinafter DBT's AutoTrackXP.com Secure, Anti-Fraud Web Site Listed].

fn77. Associated Press, DEA, FBI Suspend Online Contracts With Database Company (July 13, 1999) (document obtained from the Office of National Drug Control Policy), available at http://www.epic.org/privacy/choicepoint/cpondcp2.5.02.pdf.

fn78. See Memorandum from Joseph Peters, National Director, High Intensity Drug Trafficking Areas (HIDTA) Program, Bureau of State and Local Affairs, Office of National Drug Control Policy, to All HIDTA

Directors (Jun. 17, 1999) (document obtained from the Office of National Drug Control Policy), available at http://epic.org/privacy/choicepoint/cpondcp2.5.02.pdf.

fn79. Memorandum from H. Marshall Jarrett, Counsel, DOJ, to Kenneth L. Wainstein, Director, Executive Officer for United States Attorneys (Jun. 17, 2002) (document obtained from the DOJ), available at http://epic.org/privacy/choicepoint/cpdoj12.13.02.pdf.

fn80. Id.

fn81. Id.

fn82. See id.

fn83. See id.

fn84. Memorandum from Robert J. Finan II, Assistant Director, Investigative Services Division, USMS, to All United States Marshals, All Chief Deputy United States Marshals, and All Warrant Supervisors (Feb. 19, 1999) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn85. Id.

fn86. Id.

fn87. Memorandum from Robert J. Finan II, Assistant Director, Investigative Services Division, USMS, to All United States Marshals, All Chief Deputy United States Marshals, and All Warrant Supervisors (Jan. 28, 1999) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn88. Letter from Database Technologies, Inc. to Intelligence Analyst, USMS (Oct. 9, 1997) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02a.pdf.

fn89. Letter from James Milford, Vice President, Database Technologies, Inc., to the USMS (May 29, 1998) (document obtained from the USMS) (emphasis in original), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf.

fn90. Id.

fn91. USMS, Past Performance Work Sheet (Nov. 20, 2000) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02a.pdf.

fn92. ChoicePoint, ChoicePoint International Data Access Statement of Work: U.S. INS (Sept. 12, 2001) (document obtained from the INS), available at http://epic.org/privacy/choicepoint/cpins3.25.02b.pdf [hereinafter ChoicePoint International Data Access Statement of Work].

fn93. Id.

fn94. 15 U.S.C. 78dd-1, 78dd-2, 78m(b), 78ff (2000).

fn95. Memorandum of the INS (n.d.) (document obtained from the INS), available at http://epic.org/privacy/choicepoint/cpins3.25.02a.pdf.

fn96. INS, Independent Government Cost Estimate for On-Line International Public Access (n.d.) (document obtained from the INS), available at http://epic.org/privacy/choicepoint/cpins3.25.02a.pdf; INS, ChoicePoint (n.d.) (document obtained from the INS) available at http://epic.org/privacy/choicepoint/cpins3.25.02a.pdf [hereinafter Choicepoint (INS)].

fn97. Choicepoint (INS), supra note 96.

fn98. Id.

fn99. Generally, American state laws protect personal information in voting registers, and only allow candidates to use the information for campaigning. See, for instance, Maryland's code on the subject: "Any individual who knowingly allows a registration list under the individual's control to be used for commercial solicitation or any other purpose not related to the electoral process is guilty of a misdemeanor and shall be punished under the provisions of Title 16 of this article." Md. Code Ann., Elect. 3-507(c) (2000).

fn100. ChoicePoint International Data Access Statement of Work, supra note 92.

fn101. Id.

fn102. Id.

fn103. See Jim Krane, U.S. Buys Latin Americans' Personal Data, Seattle Times, Apr. 14, 2003, at A10, available at http://www.seattletimes.com (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn104. Ricardo Chavira, Firm: Mexican Voters' Data Illegally Obtained: Atlanta Company Says It Violated No Law, Blames Vendor, Will Purge Files, Dallas Morning News, May 17, 2003, at 21, available at http://www.dallasnews.com/sharedcontent/dallas/world/stories/051703dnintvote.edb9.html.

fn105. Argentinian privacy expert Pablo A. Palazzi tracked the ChoicePoint sale reaction closely. See Pablo A. Palazzi, Data Protection Materials in Latin American Countries (June 30, 2003), available at http://www.ulpiano.com/DataProtection-LA-links.htm.

fn106. Latin American Officials Demand Investigation Into Data Sales, USA Today, Apr. 16, 2003 [hereinafter Investigation Into Data Sales].

fn107. Hugh Dellios, U.S. Data Mining Investigated; "Information Trafficking' Riles Latin America, Chi. Trib., Oct. 12, 2003, at 6.

fn108. Oliver Burkeman & Jo Tuckman, How US Paid For Secret Files on Foreign Citizens: Latin Americans Furious in Row Over Selling Personal Data, Guardian, May 5, 2003, at 4.

fn109. Investigation Into Data Sales, supra note 106.

fn110. Peralte C. Paul & Susan Ferriss, Privacy Concern Crosses Boundary; Mexican Government Says Alpharetta-based ChoicePoint Illegally Sold Voter Data to U.S., Atlanta J.-Const., Apr. 27, 2003, at 1Q.

fn111. Associated Press, House Arrest For 3 Suspected Of Selling Mexico Voter Data (Nov. 25, 2003), available at http://www.ap.org (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn112. News Articles (various dates) (documents obtained from the Department of State), available at http://epic.org/privacy/choicepoint/cpdos11.3.03.pdf.

fn113. Department of State, Action Cable: Media Hammers U.S. on Alleged Purchase of Database Information, (Apr. 15, 2003) (document obtained from the Department of State), available at http://epic.org/privacy/choicepoint/cpdos12.3.03.pdf.

fn114. Id.

fn115. Id.

fn116. Id.

fn117. E-mail from William Peters to Reference at IIP (Apr. 28, 2003) (document obtained from the Department of State), available at http://epic.org/privacy/choicepoint/cpdos2.2.04.pdf.

fn118. Id.

fn119. Costa Rica Pres to Propose Limits on Sale of Databases, Wall St. J., Aug. 7, 2003, available at http://online.wsj.com/article/0,,BT_CO_20030805_009404,00.html (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn120. ChoicePoint Said to Stop Selling Data on Mexicans to US, Wall St. J., Aug. 31, 2003, available at http://online.wsj.com/article/0,,BT_CO_20030831_000609,00.html (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn121. ChoicePoint International Data Access Statement of Work, supra note 92.

fn122. Dep't of the Treasury, Justification for Other Than Full and Open Competition (Apr. 9, 2002) (document obtained from the Dep't of the Treasury), available at http://epic.org/privacy/choicepoint/cpatf4.9.02a.pdf.

fn123. Id.

fn124. DBT's AutoTrackXP.com Secure, Anti-Fraud Web Site, supra note 76.

fn125. See Dep't of the Treasury, Reimbursable Agreement (July 28, 2000) (document obtained from the Dep't of the Treasury), available at http://epic.org/privacy/choicepoint/cpatf4.9.02a.pdf.

fn126. The FOIA has a provision that allows the government not to reveal the presence of classified documents that are secret. 5 U.S.C. 552(c)(3) (2000). When individuals request such material, the agency may respond that it has no responsive records. See id.

fn127. See Memorandum from the Criminal Investigative Division, FBI, to the Finance Division, FBI (Apr. 4, 2000) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbi1.31.02a.pdf.

fn128. FBI, Justification for Other Than Full and Open Competition (n.d.) (document Obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbi1.31.02b.pdf.

fn129. Letter from Jennifer Paisner, Trial Attorney, DOJ, to Chris Hoofnagle, Deputy Counsel, Electronic Privacy Information Center (Apr. 29, 2003) (on file with author).

fn130. See Defendant's Motion to Exclude Classified Documents from Plaintiff's FOIA Request, Elec. Privacy Info. Ctr. v. DOJ, No. 02-0063 (D.D.C. 2002) (filed Dec. 31, 2003).

fn131. FBI, Schedule (Nov. 27, 2000) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbi1.31.02a.pdf.

fn132. FBI, Non Disclosure Agreement: Rough Draft (July 7, 2000) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbi1.31.02c.pdf.

fn133. Id.

fn134. Id. (providing at paragraph H.7(5)(a), Secret Security Clearances, that "all Owners, officers, directors, executive personnel, job superintendents, and security officers of the Contractor and selected subcontractors with access to the FBI Facility or to the contract documents shall possess ... clearances at the "SECRET" level").

fn135. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

fn136. Memorandum from Office of the General Counsel, National Security Law Unit, FBI, to National Security, FBI (Sept. 17, 2001) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbia.pdf [hereinafter Memorandum from Office of the General Counsel].

fn137. Id. (emphasis in original).

fn138. FBI, Office of the General Counsel, National Security Law Unit, Routing Slip (Sept. 16, 2001) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbic.pdf.

fn139. James Dempsey & Lara Flint, Ctr. for Democracy & Tech., Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data 1 (2003), available at http://www.cdt.org/security/usapatriot/030528cdt.pdf.

fn140. 15 U.S.C. 1681a-t (2000).

fn141. U.S. Const. amend. IV.

fn142. Katz v. United States, 389 U.S. 347, 350 (1967).

fn143. Id. at 361.

fn144. United States v. Miller, 425 U.S. 435, 442 (1976).

fn145. Dempsey & Flint, supra note 139, at 3.

fn146. See Phil Brennan, National Security Becomes National Snoopery, NewsMax.com (Apr. 24, 2002), at http://www.newsmax.com/archives/2002/4/23/162051.shtml; Sarah Lai Stirland, Reluctant Snoops: For Internet Services, War Against Terror Means Flood of Subpoenas, SeattleTimes.com (Sept. 30, 2002), at http://archives.seattletimes.nwsource.com (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn147. Brennan, supra note 146.

fn148. Yuval Dror, Big Brother Is Watching You - and Documenting, HaaretzDaily.com (Feb. 20, 2003) (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn149. Id.

fn150. Id.

fn151. See Right to Financial Privacy Act of 1978, 12 U.S.C. 3401-3422 (2000). A detailed description of the Act is available at http://epic.org/privacy/rfpa/.

fn152. Most recently, a New Jersey Appellate Court rejected Miller, and now the government in that state must obtain a search warrant to obtain access to financial records. See State v. McAllister, 840 A.2d 967, 976, 978 (N.J. App. Div. 2004).

fn153. DOJ, Blanket Purchase Agreement for Access to Public Databases (n.d.) (document obtained from the DOJ), available at http://epic.org/privacy/choicepoint/cpdoj8.14.02.pdf.

fn154. Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. 552a (1994)). A detailed description of the Act is available at http://epic.org/privacy/1974act. See also Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 Stan. Tech. L. Rev. 1 (2001) (providing a discussion of the Privacy Act).

fn155. 5 U.S.C. 552a.

fn156. Id. 552a(m).

fn157. USMS, Modification: M001 (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf.

fn158. 5 U.S.C. 552a(m)(2).

fn159. Id. 552a(k).

fn160. 15 U.S.C. 1681a-t (2000). A detailed description of the Act is available at http://epic.org/privacy/fcra/.

fn161. Id. 1681b (2000).

fn162. Id. 1681b(a).

fn163. Id. 1681u.

fn164. Pub. L. No. 107-56, 115 Stat. 272 (2001).

fn165. Id. 1681v (Supp. 2001).

fn166. Id. 1681f.

fn167. Id. 1681a(d) (emphasis added).

fn168. Memorandum from Office of the General Counsel, supra note 136.

fn169. Id.

fn170. Dempsey & Flint, supra note 139, at 6 n.16.

fn171. Interactive Pager Service Agreement, supra note 35.

fn172. DOJ, Reimbursement Agreement Between Agencies (Apr. 8, 2002) (document obtained from the DEA), available at http://epic.org/privacy/choicepoint/cpdea7.3.02.pdf [hereinafter Reimbursement Agreement Between Agencies].

fn173. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at scattered sections of 12, 15, 16, 18 U.S.C.). A detailed description of the Act is available at http://epic.org/privacy/glba/.

fn174. 15 U.S.C. 6801 (2000).

fn175. Id. 6802(e)(5).

fn176. Id.

fn177. Id. 6806.

fn178. Id. 6801(b), 6809.

fn179. Id. 6802(c)-(d).

fn180. 18 U.S.C. 2721-2725 (2000).

fn181. Id. 2721.

fn182. See id.

fn183. Pricing Schedule D, supra note 31.

fn184. Two of the lawsuits, Levine v. Reed Elsevier, No. 03-80490 (S.D. Fla. filed May 30, 2003) and Levine v. ChoicePoint, No. 03-80491 (S.D. Fla. filed May 30, 2003) have been dismissed. Brooks v. Auto Data Direct, No. 03-61063 (S.D. Fla. filed May 29, 2003) is still being litigated.

fn185. See SWIPE Project (produced by Beatriz da Costa, Jamie Schulte and Brooke Singer), at http://www.we-swipe.us/ (last visited Mar. 27, 2004).

fn186. Reimbursement Agreement Between Agencies, supra note 172.

fn187. A thorough review of the Principles exceeds the scope of this article. For such a review, see Fed. Trade Comm'n, Individual Reference Services: A Report to Congress (Dec. 1997), available at http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

fn188. Individual Reference Services Group, IRSG Principles (2003), available at http://west.thomson.com/bottom/irsgprin.asp [hereinafter IRSG Principles].

fn189. Id.

fn190. Id.

fn191. Letter from Gina Moore, ChoicePoint, to Chris Hoofnagle, Electronic Privacy Information Center (Feb. 21, 2003) (emphasis in original) (on file with author).

fn192. David Gram, Associated Press, Vt. Bookseller Purges Files to Avoid Potential "Patriot Act' Searches (Feb. 20, 2003), available at www.ap.org (on file with the North Carolina Journal of International Law and Commercial Regulation). Bookstores have also fought law enforcement access to book purchasing records with success before the passage of the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272, tit. X (2001). One example is the Monica Lewinsky case and Tattered Cover. See, e.g., Steven K. Paulson, Associated Press, Colorado Supreme Court Refuses to Order Book Store to Turn Over Sales Records (Apr. 8, 2002), available at www.ap.org (on file with the North Carolina Journal of International Law and Commercial Regulation) (reporting on Tattered Cover).

fn193. See, e.g., Paul W. Valentine, Md. Drivers Rushing to Seal Records, Wash. Post, Dec. 1, 1997, at A1 (documents obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf; Frank J. Murray, Justices Uphold Privacy Law As Way to Protect Motorists: Rule Congress Can Ban Sale of License Information, Wash. Post, Jan. 13, 2000, at A3, (documents obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf.

fn194. Fact Versus Fiction, supra note 12.

fn195. Id.

fn196. Memorandum to All Executives and Managers, supra note 25.

fn197. E-mail from Doug Dyer, Lt. Col., DARPA/IAO, to John Poindexter & Robert Popp, DARPA/IAO (May 26, 2002) (document obtained from the Department of Defense), available at http://www.epic.org/privacy/profiling/tia/darpaacxiom.pdf [hereinafter E-mail from Doug Dyer].

fn198. Total Information Awareness is a now-defunct plan of the Department of Defense where the agency had planned to use ultra-large databases to find leads on criminal behavior.

fn199. E-mail from Doug Dyer, supra note 197.

fn200. Id.

fn201. Id.

fn202. Direct Marketing Association, Guidelines for Ethical Business Practice, available at http://www.the-dma.org/guidelines/ethicalguidelines.shtml#collect (last revised Oct. 2003).

fn203. A Matter Of Privacy, Delaney Rep. (Informed Communications, Inc., New York, New York), Vol. 4, No. 34 (Aug. 30, 1994), available at 1993 WL 2870174.

fn204. The DMA did reserve the right to use public records for any purpose. See Direct Mktg. Ass'n, Written Comments of The Direct Marketing Association Before the Federal Trade Commission (Apr. 15, 1997) (FTC Docket Nos. Database Study P974806, Consumer Privacy P954807) available at http://www.ftc.gov/bcp/privacy/wkshp97/comments2/dma.htm.

fn205. See George Orwell, 1984 (1949).

fn206. Sole Source Justification for Autotrack (Database Technologies), supra note 1.

fn207. Access and Aggregation, supra note 2, at 1145-49; see also Roger Clarke, Privacy and "Public Registers' (May 11, 1997), available at http://www.anu.edu.au/people/Roger.Clarke/DV/PublicRegisters.html; Robert Gellman, Public Records: Access, Privacy, and Public Policy (May 16, 1995), available at http://www.cdt.org/privacy/pubrecs/pubrec.html.

fn208. Robert Ellis Smith, Here's Why People Are Mad, Vol. 29, No. 3 Privacy J. 7, 7 (Jan. 2003) (citing Stephen Grimes, administrator of the Judicial Records Center in Rhode Island), available at http://www.privacyjournal.net/ (on file with the North Carolina Journal of International Law and Commercial Regulation).

fn209. Id.

fn210. ChoicePoint International Data Access Statement of Work, supra note 92.

fn211. Pricing Schedule D, supra note 31.

fn212. Id.

fn213. Sec'y Advisory Comm., Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973), available at http://www.epic.org/privacy/hew1973report/c2.htm; see Personal Privacy in an Information Society, supra note 4.

fn214. See Orwell, supra note 205.

fn215. Daniel Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393, 1398 (2001).

fn216. See 5 U.S.C. 552a(m) (2000).