Breaking the Congressional Logjam: A New Approach to the Regulation of Commercial Data Brokers

Bradley J. Schaufenbuel
The John Marshall Law School
June 2008

Abstract

This paper discusses the commercial data brokerage industry, the current legal and regulatory framework that governs it, and the events that led to recognition of its threat to consumer privacy. I then examine what federal and state legislatures have (and have not) accomplished in the wake of the Choicepoint and Lexis Nexis security breaches. Finally, I propose a regulatory framework that will break the congressional logjam by addressing the concerns of both consumer privacy advocates and the commercial data brokerage industry based on a concept borrowed from the regulation of banks and insurance companies - the "optional federal charter".

Background

Commercial Data Broker Business Overview

There are more than 1,000 commercial data brokers (CDBs) in the United States.[1] The basic business model of CDBs consists of three main activities. CDBs collect personally identifiable information from a plethora of sources, including public records (such as property tax records, recorded deeds, etc.), publicly available information (such as telephone directories), and non-public information (such as information provided by customers to obtain services).[2] CDBs then create individual “dossiers” by aggregating, organizing, and indexing this vast amount of personally identifiable information by individual.[3] Finally, these dossiers are distributed to a wide variety of customers, including lawyers, law enforcement agents, reporters, landlords, intelligence and homeland security officials, and employers.[4]

Choicepoint, for example, is the largest CDB in the United States. It has collected more than 19 billion records and has purchased a large number of smaller data collection companies that obtain everything from criminal history records and insurance claims to databases of DNA signatures.[5] The private sector (banks, insurance companies, lenders, etc.) and increasingly law enforcement officials rely on the information provided by Choicepoint to help them decide whether Americans are hired, get home loans, pass background checks, obtain insurance, and qualify for public contracts.

Generally, companies or government agencies purchase information about an individual from CDBs and this information usually includes the data subject's Social Security number.[6] Customers of CDBs conduct the vast majority of these transactions via the web rather than in person.[7] The anonymity of most CDB transactions has opened the door for criminals to pose as legitimate businesses and obtain vital information about an individual. The criminal then uses the information to steal the data subject's identity. For example, the Washington Post featured an article about a band of identity thieves who used stolen credit card numbers and consumer reports they obtained from a CDB to piece together enough information about the victims to transfer funds from the victims’ accounts, write phony checks against those accounts, etc.[8]

Current Legal and Regulatory Regime

Piecemeal Implementation

As Deborah Majoras, Chairman of the Federal Trade Commission, notes, “[t]here is no single federal law that governs all uses or disclosures of consumer information.”[9] Federal privacy protection is limited to

discrete sectors and concerns because, in most cases, “Congress has simply reacted to public scandals.”[10] Thus, instead of creating comprehensive regulations for CDBs, federal legislation only focuses on punishing abuses as they arise.[11] Aside from scattered federal laws, some state legislation exists to help minimize the privacy risks associated with CDBs. In fact, states have been generally more direct and innovative in their legislation of CDBs. However, the protections involved with state legislation are very inconsistent.

Exceptions and Loopholes

Because of the piecemeal nature of legislation, CDBs have been able to take advantage of the loopholes that permeate these laws. CDBs often cite the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) as providing regulatory oversight of their operations. However, each of these acts contains imprecise definitions and broad exceptions that CDBs exploit to limit the law's applicability to them. In fact, CDBs structure their operations to avoid privacy protection laws that restrict information gathering and sharing by government agencies and credit bureaus.[12]

The FCRA, for example, focuses on the oversight of credit reporting agencies. The FCRA prohibits, with several listed exceptions, the distribution of “consumer reports” by “consumer reporting agencies” except for “permissible purposes,” while ensuring that the consumer reporting agencies make reasonable efforts to verify the identity of prospective recipients.[13]

The FCRA defines "consumer reports" as reports that contain information that is collected and sold to commercial businesses to facilitate consumer related decisions.[14] The FCRA governs CDBs only to the extent that the FTC considers the information they distribute to be a "consumer report". To distribute “consumer reports,” a credit-reporting agency must meet one of the "permissible purposes" that is defined in the FCRA.[15] Most relevant to the distribution of data by CDBs, however, is that under the FCRA, CDBs may provide reports to a business to make credit, insurance, or employment decisions. Yet another loophole that CDBs may take advantage of is that credit reporting agencies or CDBs may also distribute consumer reports to a person or organization that has a broadly defined "legitimate business need".[16]

The limiting nature of the term “consumer reports” and the substantial number of exceptions that the FCRA provides does not leave the public with much privacy protection.[17]

The GLBA, which Congress passed back in 1999, limits the type of information that “financial institutions” can distribute. The GLBA prohibits financial institutions from disclosing "nonpublic personal information" (NPPI) to non-affiliated third parties without first notifying the customer of the disclosure and allowing them an opportunity to opt out of the disclosure.[18]

The GLBA governs CDBs to the extent that they fall under the “financial institution” classification. However, there are exceptions under which a financial institution is not required to follow the notice guidelines of the GLBA. If the CDB obtains information pursuant to a GLBA exception, it can only use this information “in the ordinary course of business to carry out the activity covered by the exception under which it received the information.”[19]

Under a GLBA exception, credit reporting agencies and CDBs frequently receive “credit header information” from various financial institutions, consisting of a person’s name, address, and Social Security number. Whether or not the CDB receives the information directly from the financial institution, or from a credit-reporting agency who originally received the information from a financial institution, the CDB is subject to the requirements of the GLBA.[20]

While these laws may create obstacles for the CDBs to conduct their business, none of them has been particularly effective in preventing the mistaken distribution of people’s personally identifiable information to identity thieves.[21]

Focus on Governmental Use

A unique characteristic of U.S. privacy law is the focus on protection against public incursion.[22] U.S. privacy legislation generally provides "significantly greater protection against the collection and use of personal information by government . . . than by the private sector."[23] For instance, the Privacy Act of 1974 only applies to the activities of the federal government. In fact, "[s]hort of some highly injurious or offensive use, corporations can use personal information about customers in almost any manner they believe might be profitable."[24] Consequently, as private corporations, CDBs are essentially unregulated in their collection, use, and sale of individuals' personally identifiable information.[25]

Data Subject Awareness

U.S. privacy protection laws do not require CDBs to notify individuals of the existence of the dossier they have created on them[26]. Most Americans may be completely unaware of how much of her lives CDBs have recorded in databases[27] because the United States "does not require an individual's consent to the processing, marketing, and sale to third parties of personal information."[28]

Inaccuracy

Although studies have shown that at least some of the information in almost all of the dossiers created by CDBs is inaccurate and that these errors have adversely impacted individuals, CDBs are not accountable for inaccuracies in the dossiers they sell.[29]

Enforcement

Even where data brokers are governed by existing U.S. legislation, "no central administrative agency monitors compliance."[30] Consequently, "even where legal coverage exists, there is insufficient enforcement, consumers find it difficult to exercise their rights, and the auditing of their activities is non-existent."[31]

Common Law

In the absence of effective federal legislation, the common law currently offers little in the way of remedies to individuals whose personal data is misused. Contract solutions have failed because it is tough for consumers to enforce the privacy agreements of the companies they do business with – if those companies even have privacy agreements.[32] Scholars who have pondered a remedy in tort for the mis-use of information have largely concluded that the existing set of privacy torts is woefully inadequate.[33]

Remedies

CDBs are not legally liable for any misuses of the information they sell.[34] Individuals whose data has been misused have few viable statutory remedies. Many federal privacy statutes do not include provisions that grant a private right of action, or provide such a paltry level of liquidated damages that suing CDBs is not cost effective.[35]

Self-regulatory Regime

The government's relatively passive role in privacy protection has "historically been predicated on the philosophy that self-regulation will accomplish the most meaningful protection of privacy without intrusive government interference, and with the greatest flexibility for dynamically developing technologies."[36] According to this theory, "the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers . . . [and] industry will seek to protect personal information in order to gain consumer confidence and maximize profits."[37]

IRSG – Individual References Services Group

In the absence of statutory regulation, CDBs adopted self-regulatory rules known as the Individual Reference Services Group (IRSG) Principles. The principles created a weak framework of protections, allowing CDBs to sell non-public personally identifiable information "without restriction" to "qualified subscribers," a category of customers which included most government agencies.[38] "Qualified subscribers" need only have communicated a "valid purpose" for obtaining the information (which CDBs were not required to verify) and agree to limit re-dissemination. Under the IRSG principles, individuals could only opt-out of the distribution of personally identifiable information to the "general public." However, CDBs did not consider their customers to be a part of the "general public".

CDBs carefully constructed the IRSG Principles in order to ensure themselves maximum flexibility. They failed to create even a modest degree of privacy protection for individuals. In fact, it was while CDBs were operating under the principles that the major privacy breaches of 2005 occurred.[39] Interestingly, the Individual Reference Services Group appears to be defunct. Its website, http://www.irsg.org, now contains an advertisement for plastic surgery.

The Events of 2005 – The Choicepoint and Lexis Nexis Breaches

In February 2005, Choicepoint divulged to tens of thousands of Californians that it had sold their personally identifiable information, including "names, addresses, Social Security numbers, [and] credit reports," to a ring of identity thieves who had registered phony companies – using previously stolen identities – for the purpose of purchasing the information.[40] Choicepoint eventually revealed that it sold the personally identifiable information of more than 163,000 people, but declined to specify to the affected consumers exactly what data it had sold.[41]

In March 2005, Lexis Nexis announced that criminals might have accessed the personally identifiable information of 32,000 people, including first and last names, addresses, Social Security numbers, and driver's license numbers, through its subsidiary, Seisint.[42] After completing its security review, LexisNexis increased its estimate, concluding that criminals had accessed the personal information of 310,000 people in fifty-nine separate incidents of security breaches.[43]

Subsequent Calls for the Regulation of the Commercial Data Brokerage Industry

The massive data security breaches at Choicepoint and Lexis Nexis were the tipping point. Since the news of these breaches broke, the data brokerage industry as well as the privacy and security of personally identifiable information (PII) have been subject to increasing public and congressional attention.[44]

Both the House of Representatives and the Senate held hearings in the spring of 2005 to discuss the Choicepoint and Lexis Nexis breaches and to consider the need for legislative action. Derek Smith, the CEO of Choicepoint, as well as privacy advocates such as a representative from the Electronic Privacy Information Center (EPIC) and a representative from the Center for Democracy and Technology (CDT), testified. Following these hearings, Congressional action seemed imminent.

Regulatory Proposals - What has Transpired Since

Following the Choicepoint and Lexis Nexis debacles, the CDB industry pushed for legislation focusing mostly on punishing the people who use their data to commit identity theft. Many members of Congress, however, believed that it was necessary to pass legislation that would regulate the manner by which CDBs collect, protect, and distribute information. With these competing interests, Congress was and still is faced with the difficult task of regulating an industry that may be placing consumers' identities at risk,

while ensuring that the legislation they pass does not unduly burden the CDBs' ability to provide important public benefits.[45]

While Congress and numerous state legislatures rapidly introduced bills to force CDBs to be more accountable to their data subjects, few states actually enacted laws, and Congress took none of the federal bills to a vote prior to the election in 2006.[46] In large part, individuals remain powerless to discover the information that a CDB has collected about them, to discover what information CDBs have sold to others about them, to prevent CDBs from using their personally identifiable information in an unauthorized manner, or to hold CDBs accountable for poor data security practices. A breakdown of legislative activity follows.

Federal Bills

Members the United States House and Senate introduced numerous bills dealing with data security in the spring of 2005. Many of them included notification requirements, security freezes, and access for individuals to their data files. Various bills called for increased FTC oversight and regulation of CDBs and further restrictions on the legal uses of Social Security numbers. Two bills proposed a private right of action for individuals. Several bills specified that federal legislation would preempt any state laws governing CDBs, which prompted substantial criticism from privacy advocates that the softer federal legislation would destroy the stronger efforts of states like California and Massachusetts to protect the privacy of their citizens.[47] After getting off to a rapid start, every one of the bills ended up mired down in committees by turf wars and intense lobbying.[48] None became law in 2005, and although some of the bills have actually emerged from committees, neither the 109th nor the 110th Congress has passed any of them. The following tables identify all of the bills.

109th Congress (2005 – 2006)[49]

Bill Number	Title	Sponsor
S. 29	Social Security Number Misuse Prevention Act	Sen. Feinstein (D-CA)
S. 115	Notification of Risk to Personal Data Act	Sen. Feinstein (D-CA)
S. 116	Privacy Act of 2005	Sen. Feinstein (D-CA)
H.R. 220	Identity Theft Prevention Act of 2005	Rep. Paul (R-TX)
S. 500	Information Protection and Security Act	Sen. Nelson (D-FL)
S. 751	Notification of Risk to Personal Data Act	Sen. Feinstein (D-CA)
S. 768	Comprehensive Identity Theft Prevention Act	Sen. Schumer (D-NY)
H.R. 1080	Information Protection and Security Act	Rep. Markey (D-MA)
H.R. 1078	Social Security Number Protection Act of 2005	Rep. Markey (D-MA)
H.R. 1263	Consumer Privacy Protection Act of 2005	Rep. Stearns (R-FL)
S. 1326	Notification of Risk to Personal Data Act	Sen. Sessions (R-AL)
S. 1332	Personal Data Privacy and Security Act of 2005	Sen. Specter (R-PA)
S. 1408	Identity Theft Protection Act of 2005	Sen. Smith (R-OR)
H.R. 1745	Social Security Number Privacy and Identity Theft Prevention Act of 2005	Rep. Shaw (R-FL)
H.R. 3140	Consumer Data Security and Notification Act	Rep. Bean (D-IL)
H.R. 3374	Consumer Notification and Financial Data Protection Act of 2005	Rep. LaTourette (R-OH)
H.R. 3375	Financial Data Security Act	Rep. Pryce (R-OH)
H.R. 3501	Consumer Access Rights Defense Act (CARD) of 2005	Rep. Carson (D-IN)
H.R. 4127	Data Accountability and Trust Act	Rep. Stearns (R-FL)

110th Congress (2007 – 2008)[50]

Bill Number	Title	Sponsor
S. 495	Personal Data Privacy and Security Act of 2007	Sen. Leahy (D-VT)
H.R. 958	The Data Accountability and Trust Act	Rep. Rush (D-IL)
S. 239	Notification of Risk to Personal Data Act of 2007	Sen. Feinstein (D-CA)
H.R. 836	The Cyber-Security Enhancement and Consumer Data Protection Act of 2007	Rep. Lamar (R-TX)
H.R. 948	Social Security Number Protection Act of 2007	Rep. Markey (D-MA)
H.R. 4175	Privacy and Cybercrime Enforcement Act of 2007	Rep. Conyers (D-MI)
S. 239	Notification of Risk to Personal Data Act of 2007	Sen. Feinstein (D-CA)
S. 1178	Identity Theft Prevention Act	Sen. Inouye (D-HI)
S. 1208	Social Security Account Number Protection Act	Sen. Dorgan (D-ND)
S. 1202	Personal Data Protection Act of 2007	Sen. Sessions (R-AL)
H.R.1685	Data Security Act of 2007	Rep. Pryce (R-OH)
S. 238	Social Security Number Misuse Prevention Act	Sen. Feinstein (D-CA)

State Bills

The state legislatures were much more successful than Congress, with notification provisions faring the best. Before the Choicepoint and Lexis Nexis breaches, only California required CDBs to notify individuals of security breaches. By mid-2006, thirty-three states had passed laws requiring notification to consumers of data security breaches, but similar legislation had failed to pass in thirteen other states, including a proposal in California to strengthen the existing law.[51] By mid-2006, security freezes had been enacted in twenty-five states, but were debated and floundered in ten other states (including proposals in California and Texas to enhance existing laws). Five states – Colorado, Louisiana, New Jersey, North Carolina, and Rhode Island – enacted laws that create a private cause of action for consumers when CDBs violate their notice or freeze obligations.[52]

The Preemption Issue

The federal proposals call for differing levels of preemption. Some bills would totally preempt state laws that cover data security, breach notification, identity theft, and other consumer-privacy issues. Other bills, however, while preempting state privacy laws in the categories of data security and breach disclosure, would allow states to continue to legislate in other categories of information assurance and protection as long as the state laws were consistent with the federal law, in a manner similar to the GLBA.[53]

The question of the relationship of federal legislation to state data breach notification, data security, and credit freeze laws was paramount in both the 109th and 110th sessions of Congress. CDBs and their lobbyists expressed concerns that multiple state laws make compliance an overly complex task.[54] In fact, the lack of preemption is one of the main reasons why Congress failed to pass a federal law regulating CDBs.

The Way Forward – An Optional Federal Charter for CDBs

After 31 failed attempts at federal regulation of CDBs in three years, it is clear that resolving this problem requires a fresh approach. To design a better legislative proposal – one that has a reasonable chance of being enacted by Congress – one must examine the roadblocks to implementation and consider how people have already addressed similar problems in other industries.

Preemption – The Roadblock to Progress

I first consider what the critical roadblock to implementation of federal legislation to regulate CDBs is. That requires an examination of why CDBs have lobbied so intensely against the federal proposals. Much of the contention between CDB lobbyists and consumer privacy advocates has been over the preemption issue. The biggest fear of the CDBs appears to be that they will end up having to deal not only with a patchwork of fifty plus ever-changing and aggressive state regulations, but with an overlapping set of federal regulations as well.

On the other side of the fence, privacy advocates have lobbied hard against the inclusion of preemption clauses in any of the federal data privacy bills. They are afraid that a federal law with weak privacy protections and a preemption clause will wipe out all of the strong and innovative measures that state legislators have already successfully enacted.

We Have Crossed This Bridge Before

This is not the first time in U.S. history where a series of events that negatively affected consumers led to calls for the regulation of an industry, the industry resisted, and the response by both state legislators and Congress resulted in a confusing patchwork of conflicting legislation. A similar scenario played out during the banking crisis of the 1930s and is playing out in the insurance industry today. The solution that Congress successfully deployed in the former case and that it is currently considering in the latter case is the implementation of an "optional federal charter" (OFC) regulatory framework.

The Optional Federal Charter

The essence of my proposal to break the congressional logjam is the implementation of an optional federal charter regulatory framework for the CDB industry. To understand the OFC concept, one must understand its essential features, its administration, its funding model, its effects on state legislation, and the restraints that ensure that it balances the needs of the regulated with those who have a stake in regulation.

Essential Features of the Plan

The essential features of an optional federal charter regulatory scheme would be as follows. First, the federal charter program would be optional / voluntary. CDBs would not have to join. Second, optional federal chartership would be reversible. Once a CDB has opted into the OFC framework, it would be able to exit and / or rejoin the program at any time. However, enforcement actions against CDBs would continue regardless of subsequent changes in charter status. Finally, federal chartership would result in state regulatory preemption. While CDBs hold a federal charter, they would be exempt from the states' data privacy regulations. If CDBs choose not to join, they will continue to be subject to states' data privacy regulations.

Administration

The enabling legislation creating the optional federal charter program would require the chairperson of the Federal Trade Commission to appoint a national privacy commissioner (similar to the European Data Privacy Directive's requirement that member nations appoint a similar official). The office of the privacy commissioner would administer the OFC program (including oversight of the granting and revocation of charters, the execution of supervisory duties, and instigation of enforcement actions). Congress would grant the office of the privacy commissioner broad rule making authority in the area of data privacy and the regulation of CDBs.

Funding

The office of the privacy commissioner would partially fund itself through charter fees and partially fund itself through fines levied against CDBs found to be non-compliant with the rules and regulations it promulgates. Congress would not burden the American taxpayer by having to fund another federal regulatory agency.

Constraints on Over and Under Regulation

The self-funding mechanism of charging charter fees would encourage the privacy commissioner to set regulations that are not so stringent that CDBs do not wish to join the program. The self-funding mechanism of fines would encourage the office of the privacy commissioner to enforce its regulations (to pay for its operations). The collection of fines as a self-funding mechanism would encourage the office of the privacy commissioner to set regulations that are not so weak that CDBs can easily subvert them. The optional nature of the charter would discourage the office of the privacy commissioner from being overly aggressive in the enforcement its rules and regulations. The optional nature of the charter would also discourage the office of the privacy commissioner from over-regulating the CDBs. Similar to the Digital Millennium Copyright Act, the activities of the office of the privacy commissioner would be subject to a bi-annual review in hearings open to the public, the CDB industry, and consumer privacy advocates.

Effects on State Innovation

The OFC scheme still allows the states to innovate since it does not preempt from states' data privacy legislation CDBs that opt out of the federal charter. Innovation in the states allows the federal regulator to tighten regulations because as long as the federal regulations are equally tight, the simplicity of complying with one set of rules would still encourage CDBs to hold a federal charter. The existence of the OFC program would discourage state legislators from enacting laws that are too strict, lest all of the CDBs opt for the federal charter and the law becomes moot.

Baseline Requirements

To ensure buy-in by privacy advocates and consumer groups, the enabling legislation for the OFC would require the office of the privacy commissioner to promulgate at least ten rules (what I call the consumer data privacy "bill of rights") covering the following areas:

1. A rule extending the requirements of the GLBA's Safeguards rule and the FCRA's robust Fair Information Practices to all of the activities of CDBs involving the handling of personally identifiable information.
2. A rule mandating data subject notification of data security breaches that incorporates many of the progressive features of already enacted legislation in the states.
3. A rule requiring strong protections in specific aspects of information security, as well as imposing a broad requirement that security practices in fact be effective and be continuously monitored for ongoing effectiveness.
4. A rule requiring CDBs to allow individuals to get a free copy of the dossier the CDB has compiled on them at least once a year (similar to the Fair and Accurate Credit Transactions Act rule that credit reporting agencies are subject to).
5. A rule granting individuals a private right of action against CDBs who misuse or fail to adequately protect their personally identifiable information.
6. A rule setting robust customer vetting requirements for the sale of personally identifiable information by CDBs.
7. A rule mandating regular independent third party information security audits of CDBs and the public reporting of the findings of these audits.
8. A rule mandating that CDBs give consumers an easy way to request amendments to the information kept about them.

9. A rule increasing the criminal penalties that prosecutors can seek for cyber-criminals and identity thieves that specifically target CDBs.
10. A rule restricting of the sale, collection, primary and secondary use, sharing, posting, and display of Social Security numbers by CDBs.

Benefits

The benefits of adopting an optional federal charter regulatory regime for CDBs are numerous. First, it promotes regulatory consistency. This makes it less expensive for CDBs to comply with regulatory requirements. A CDB can pass these savings along to its customers and ultimately the consumer. Second, to the extent that CDBs opt into the OFC, it guarantees a base level of protection for citizens of all states. This is preferable to the current regulatory environment, where a CDB must notify a citizen of California of a data security breach that puts his identity at risk but a citizen of Idaho enjoys no such benefit. Third, the OFC framework is self-funding, so no new taxpayer dollars are required. Without a state charter system, enforcement of data security laws at a state level must be funded using taxpayer money. Finally, the OFC framework is flexible, as the office of the privacy commissioner can adapt to changes in technology and the business environment by promulgating new rules much faster than Congress or state legislatures can enact new laws.

An attribute-by-attribute comparison between state regulation and the optional federal charter follows.

Features	State Regulation	Optional Federal Charter
Number of regulators	Fifty +.	One.
Uniformity of protection	Patchwork of laws provides differing levels of protection for citizens of different states.	Federal baseline ensures that citizens of all states enjoy fundamental protections.
Cost of compliance for CDBs	Higher.	Lower.
Flexibility / Speed of rulemaking	Enactment of laws is slow.	Promulgation of rules is fast.
Cost to taxpayers	Yes.	No. Self-funded through charter fees and fines.

Constitutionality

Given the recent trend of the United States Supreme Court to limit the power of Congress to legislate in areas that were traditionally the domain of the states by invalidating or narrowly construing federal laws[55], there may be a legitimate question as to whether the courts would strike down this optional federal charter for CDBs as unconstitutional. I contend that such a statute would withstand judicial scrutiny as a valid attempt to regulate interstate commerce under Article I, Section 8, Clause 3 of the United States Constitution. It would be relatively easy to make a case that the activities of the CDB industry "substantially affect" interstate commerce since businesses of all types use the information sold by CDBs in numerous cross border commercial transactions.

Conclusion

The Choicepoint and Lexis Nexis breaches illustrated the need to regulate the CDB industry to ensure the privacy and security of our personally identifiable information. Unfortunately, Congress has failed in its numerous attempts to bring about a comprehensive federal regulatory framework. This is primarily due to lobbying efforts by both the CDB industry and consumer privacy advocates, each of which has held firm to its support or opposition of state regulatory preemption. Fortunately, we can learn from the lessons of the banking and insurance industries. With those lessons emerges a creative solution with a significantly better chance of being enacted into law – the optional federal charter. The OFC – applied to the regulation of the CDB industry – provides just the right balance between the societal benefits that the CDB industry provides and the privacy protections that individuals expect and demand.

Endnotes

[1] Andrew J. McClurg, A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 Nw. U. L. Rev. 63, 65 (2003).
[2] Consumer Privacy and ChoicePoint Data Theft: Hearing Before the Subcommittee on Commerce, Trade,
and Consumer Protection of the H. Comm. on Energy and Commerce, 109th Cong. (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission).
[3] Daniel J. Solove, The Digital Person 110 (2004).
[4] Robert O'Harrow, Jr., ID Data Conned From Firm, Wash. Post, Feb. 17, 2005, at E1.
[5] Testimony of Consumer and Privacy Groups on Data Security, Data Breach Notices, Privacy and Identity Theft Before Committee on Banking, Housing and Urban Affairs The Honorable Richard Shelby, Chairman
United States Senate, 7 (22 September 2005).
[6] United States Government Accountability Office, Report to Congressional Committees: Personal Information: Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421 (April 4th, 2006).
[7] Marcia S. Smith, Congressional Research Service Report RS22082, Identity Theft: The Internet Connection.
[8] Robert O'Harrow, Jr., "Identity Thieves Thrive in Information Age," Washington Post, May 31st, 2001, at A1.
[9] Consumer Privacy and ChoicePoint Data Theft: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 109th Cong. (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission).
[10] Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 25 (2000).
[11] Nicole M. Buba, Note, Waging War Against Identity Theft: Should the United States Borrow from the European Union's Battalion?, 23 Suffolk Transnat'l L. Rev. 633, 643-44 (2000)..
[12] Paul N. Otto, et al., The Choicepoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information, The Privacy Place, 1 (2006).
[13] Id.
[14] 15 U.S.C. § 1681a.
[15] 15 U.S.C. § 1681b.
[16] Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information Before the Committee on Banking, Housing & Urban Affairs, 109th Cong. 2 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission).
[17] Chris J. Hoofnagle, Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004).
[18] 15 U.S.C. §§ 6801-09.
[19] Id.
[20] Id.
[21] Joshua Apfelroth, Regulating Commercial Data Brokers in the Wake of Recent Identity Theft Schemes, Business Law Brief, 35 (Fall 2005).
[22] Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 7, 20 (1996).
[23] Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 23 (2000).
[24] Craig D. Tindall, Argus Rules: The Commercialization of Personal Information, 2003 U. Ill. J.L. Tech. & Pol'y 181, 187 (2003).
[25] Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 7 (1996).
[26] Suzanne M. Thompson, The Digital Explosion Comes With a Cost: The Loss of Privacy, 4 J. Tech. L. & Pol'y 3, 31 (1999).
[27] James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 33 (2003).
[28] Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 26 (2000).
[29] Maeve Z. Miller, 39 Geo. Wash. Int'l L. Rev. 395 (2007).
[30] Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the

Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 26 (2000).
[31] Consumer Privacy and ChoicePoint Data Theft: Hearing Before the Subcommittee on Commerce, Trade,
and Consumer Protection of the H. Comm. on Energy and Commerce, 109th Cong. (2005) (statement of Marc Rotenberg, President, Electronic Privacy Information Center).
[32] Susan M. Gilles, Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy, 43 Buff. L. Rev. 1, 25-32, 38-39 (1995).
[33] James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 29-32 (2003)
[34] Robert O'Harrow, Jr., ID Data Conned From Firm, Wash. Post, Feb. 17, 2005, at E5.
[35] R. Bradley McMahon, After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?, 49 Vill. L. Rev. 625, 632 (2004).
[36] Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771, 774 (1999).
[37] Id.
[38] Individual Reference Services Group, Industry Principles – Commentary (December 1997).
[39] Solove, Daniel J. and Hoofnagle, Chris Jay, "A Model Regime of Privacy Protection (Version 2.0)" (April 5, 2005). GWU Law School Public Law Research Paper No. 132; GWU Legal Studies Research Paper No. 132.
[40] Bob Sullivan, Database Giant Gives Access to Fake Firms, MSNBC.com, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799.
[41] Electronic Privacy Information Center, EPIC ChoicePoint Page, http://www.epic.org/privacy/choicepoint/default.html.
[42] Press Release, Reed Elsevier, LexisNexis Investigates Compromised Customer IDs and Passwords to Seisint US Consumer Data, Mar. 9, 2005, http:// www.reed-elsevier.com/index.cfm?articleid=1258.
[43] Press Release, LexisNexis, LexisNexis Concludes Review of Data Search Activity, Identifying Additional
Instances of Illegal Data Access, Apr. 12, 2005, http://www.lexisnexis.com/about/releases/0789.asp.
[44] Paul N. Otto, et al., The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information, The Private Place, 1 (2006).
[45] Joshua Apfelroth, Regulating Commercial Data Brokers in the Wake of Recent Identity Theft Schemes, Business Law Brief, 33, 33 (Fall 2005).
[46] Sarah Ludington, Reining in the Data Traders: A Tort for the Misuse of Personal Information, 66 Md. L. Rev. 140, 140 (2006).
[47] Letter from Jeff Chester et al., Executive Director, Center for Digital Democracy, to Sen. Arlen Specter (R-Pa.) and Sen. Patrick Leahy (D-Vt.), Senate Committee on the Judiciary (Nov. 9, 2005), available at
http:// www.epic.org/privacy/choicepoint/datamarker11.09.05.html.
[48] Elana Schor, Data-protection Turf War Pleases Lobbyists, The Hill, Aug. 17, 2005, at 11, available at http:// www.hillnews.com/thehill/export/TheHill/Business/081705_data.html.
[49] S. Pierre Paret, National Council of Investigation and Security Services, available at http://www.honsinvestigations.com/Federal%20Legislation%20Update.pdf.
[50] THOMAS, Library of Congress, available at http://thomas.loc.gov/home/c110query.html.
[51] Sarah Ludington, Reining in the Data Traders: A Tort for the Misuse of Personal Information, 66 Md. L. Rev. 140, 157 (2006).
[52] Id.
[53] Sean C. Honeywill, Data Security and Data Breach Notification for Financial Institutions, 10 N.C. Banking Inst. 269, 274 (2006).
[54] "State Breach Notice Laws Have Similarities, But Significant Differences Require Attention," 89 BNA Analysis & Perspective 176 (Aug. 12, 2005).
[55] See *United States v. Lopez*, 514 U.S. 549 (1995) (striking down the Gun-Free Zones Act of 1990) and *United States v. Morrison*, 529 U.S. 598 (2000) (striking down the civil remedy provisions of the Violence Against Women Act).