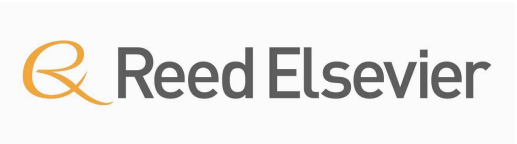

Elsevier
LexisNexis
Reed Exhibitions
Reed Business

February 18, 2011

Via Electronic Filing

Mr. Donald S. Clark
Federal Trade Commission
Room H-135 (Annex K)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

RE: Comments on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Dear Secretary Clark:

Reed Elsevier Inc. ("Reed Elsevier") appreciates this opportunity to provide comments in response to the request for public comment by the Federal Trade Commission ("FTC" or "Commission") regarding the framework for consumer privacy proposed in its December 2010 preliminary staff report (the "Report"). We commend the Commission for its continued leadership in the area of consumer privacy. The various workshops held by the Commission provided a forum for stakeholders to provide input into the complex public policy issues involving consumer privacy. Reed Elsevier commends the Commission for distinguishing within the Report between companies that interact directly with consumers and those that do not. Reed Elsevier and similar information companies have few direct consumer relationships. Unlike companies that collect information directly from consumers, Reed Elsevier relies primarily on information from government agencies and third-party data sources. Further, most products and services offered by Reed Elsevier are designed for use by business, professional, or government users.

As acknowledged in various sections of the report, attempting to apply a number of the policy recommendations to non-consumer-facing companies presents a unique set of challenges. While Reed Elsevier supports the FTC's goal of protecting consumer privacy, we have concerns with some of the key components outlined in the proposed framework, which are unworkable where information is not collected directly from consumers. We look forward to working with the Commission to address these issues as the Commission's recommendations are finalized.

I. Introduction

Reed Elsevier is one of the world's leading publishing and information companies, providing professional information solutions in the business, risk, legal and scientific sectors. Elsevier is the world's leading publisher of science and health information, publishing over 2,000 journals and close to 20,000 books and major

reference works in the scientific, technical and medical fields. Reed Business Information publishes over 400 business-to-business magazines, directories and newsletters and provides access to over 200 online communities. Reed Exhibitions is the world's foremost organizer of business-to-business trade shows, organizing over 440 events in 36 countries and attracting over six million event participants in 2009. LexisNexis is a leading provider of information products and services to the government, legal and corporate markets and serves over one million users daily. We are a critical information outlet to these users. Their reliance on LexisNexis is similar in many ways to how consumers rely on newspapers to aggregate information and distribute it to them.

All major Reed Elsevier businesses depend on the collection and use of information about persons. Medical and scientific journals published by Elsevier include information about authors and researchers and in some instances, anonymized information about selected patients or test subjects. Reed Business depends on information about persons in producing online and offline periodicals, including information about authors, interviewees and individuals in the news. Reed Exhibitions relies on access to business contact information to organize its business-to-business trade shows. LexisNexis depends on access to information to develop and update its many online and offline products including directories, news reports, court decisions and products used to help businesses and government manage risk through fraud detection and prevention, identity authentication, debt collection, and intelligent risk management and modeling.

LexisNexis products are used by businesses, non-profit organizations and government agencies for a host of important and socially beneficial purposes. Our information products and services have been donated to the National Center for Missing and Exploited Children ("NCMEC") since 2001. These information products and services have been instrumental in helping NCMEC to locate individuals that may have abducted a missing child and have helped in the recovery of hundreds of missing children. NCMEC's ability to locate and recover missing children is dependent on access to accurate, up-to-date information.

Another critical use of our products is combating sex crimes. LexisNexis helps law enforcement locate non-compliant sex offenders in order to keep our children and communities safe. LexisNexis sex offender solutions leverage content and technology to find both registered and unregistered sex offenders by street address and can map their proximity to schools, churches, day care centers, playgrounds and other areas where children congregate. Numerous state and local law enforcement agencies depend on information provided by LexisNexis in locating sex offenders who have violated registration requirements, or who may be involved in a child abduction or other offense.

LexisNexis offers numerous identity authentication and fraud detection products. Our ChargeBack Defender® product is used by merchants to prevent the use of stolen credit cards to purchase products online, over the telephone, and in other "card-not-present situations" where merchants cannot look at a credit card, check the signature, or check other identification. This product relies on data provided by consumers to merchants that is verified against data in our system to help determine whether the individual with whom the merchant is interacting is who that person purports to be. One

of the largest personal computer manufactures in the country experienced a 70% reduction in annual fraud losses by using this product.

Another example of our authentication products is Instant ID® Q&A, which is used by merchants, credit card issuers and banks to help them authenticate consumers and detect and prevent identity theft and fraud. This product uses information from many sources to develop questions that can be used to help authenticate identity. For credit card transactions specifically, the product enables retailers to verify identity information provided by a consumer before starting the credit decision process. After a top-five credit card issuer in the country began using Instant ID® Q&A, the issuer experienced a 10% reduction in annual fraud losses. This reduction in losses resulted in a net savings of more than $1 billion annually that benefited consumers by keeping down the cost of credit.

These identity confirmation and antifraud services provide tremendous benefits to consumers because our tools make it more challenging for fraudsters to use stolen identities to defraud companies and financial institutions. The victims in such frauds are consumers whose identities are stolen. Fraudsters today use very sophisticated methods. With our services those organizations seeking to prevent identity theft also have access to sophisticated tools to defeat fraud attempts.

LexisNexis also offers a number of products that are used by insurance companies to detect fraudulent property and casualty insurance claims, reducing fraud losses and reducing rates charged to consumers. In addition, LexisNexis provides products used for employment, resident and volunteer screening. These products are used to prevent harm to employees and co-workers, customers and persons in custodial care. Employers use these products to implement cost-saving fraud prevention measures and avoid liability.

II. General Comments

We applaud the Commission's recognizing the difficulty in applying certain aspects of the proposed framework to companies such as Reed Elsevier that do not collect information directly from consumers. The Report recognizes that "information brokers" who acquire consumer data from a variety of sources and do not interact directly with consumers, are not "in a position to provide consumer choice at the point of collection or use."[1] This recognition must extend to other parts of the framework that impose equally challenging burdens on businesses such as Reed Elsevier that rely upon third party sources to build and maintain their information products.

A number of the Fair Information Practice Principles ("FIPPs") simply were not designed for companies that are not obtaining information directly from consumers. As discussed above, our products are used by businesses, non-profit organizations, and government agencies for a host of important and socially beneficial purposes, including helping law enforcement locate fugitives, missing children and non-complaint sex offenders, and assisting merchants, credit card issuers, and banks with authenticating

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (December 2010), p. 63 (hereafter "Report").

consumers and detecting and preventing identity theft and fraud. While we appreciate that information used for fraud prevention and legal compliance is excluded from the choice requirements called for in the Report, such an exclusion does not apply to the other FIPPs outlined in the Report. Any policy recommendations that attempt to uniformly apply the FIPPs across all businesses will significantly harm information companies and hinder the ability of those companies to provide critical information to businesses and government agencies to detect and prevent fraud and for other important purposes, and ultimately have a negative impact on consumers.

While it has been suggested that the access and correction provisions of the Fair Credit Reporting Act ("FCRA") be expanded to apply to non-FCRA products and services, any such expansion will undermine commercial information products used for identity authentication, fraud detection and prevention, and other important purposes. The FCRA already requires consumer access and correction for the most important adverse actions, such as denials of employment, credit, insurance, or housing. We are concerned that expanding access and correction beyond what is required in the FCRA could allow information to be misused by bad actors to gain access to databases in order to "game" the system and set up fraud schemes such as "phishing" or other scams that use known information to induce consumers to reveal more compromising personal information. For example, unfettered correction or opt-out rights for a fraud and identity authentication service would allow the criminals to opt-out, manipulate or otherwise game the system. If the D.C. sniper had been allowed to opt-out of the LexisNexis Accurint service, law enforcement would not have been able to use that service to catch him.

Reed Elsevier also suggests that any effort to expand the definition of personally identifiable information ("PII") beyond those data elements that could be used to commit identity theft or fraud would represent a marked departure from an important policy distinction that different regimes in the global marketplace have embraced for decades. Many businesses, including Reed Elsevier, have built their entire business model around the distinction between PII and non-PII and have made strategic decisions in a number of critical areas based on this distinction. For some companies, these decisions have also been grounded in enforcement orders issued by the Commission that require certain actions to be taken regarding PII. Therefore, we recommend that the Commission not support an expansion of the definition of PII. Creation of uncertainty and threats of new onerous regulations changing business models will hamstring small and large American businesses alike as they seek to compete internationally.

Reed Elsevier encourages continued support of the "harm-based model," which has advanced the goal of protecting consumer privacy, is familiar to consumers, and focuses on collection and use of data that could put consumers at risk of harm. The "harm-based model" is well understood by the business community. Expanding this framework to include more undefined concepts such a "fear of being monitored," will create confusion and uncertainty and will not work well in a regulatory framework.

In describing the proposed privacy framework, the Commission recognizes that the framework does not apply to either the collection or use of data by government instrumentalities. Similarly, the privacy framework should not apply to the dissemination

of public records or the downstream use of public records or publicly available information.

Public records constitute a significant body of information on which both businesses and consumers are dependent. This information facilitates a wide range of business and consumer transactions as well as interactions between unrelated consumers and their government. For example, consumers may acquire and examine property tax records and detailed property descriptions from land, title and tax records to determine whether tax assessments against their own property are correct. Similarly, documents filed in court proceedings are used as a matter of course by others to help ensure the consumers involved in civil or criminal proceedings are treated equitably. This practice is the backbone of our precedent-based legal system.

Finally, Reed Elsevier believes that voluntary, enforceable industry codes of conduct are an effective way to address consumer privacy concerns without unfairly burdening the business community. Industry self-regulatory efforts are capable of addressing current and future privacy issues in a way that is more flexible and nimble than legislative or regulatory mandates. It is important that industry self-regulatory efforts, such as the Self-Regulatory Principles for Online Behavioral Advertising be given an opportunity to work before legislative or regulatory approaches are pursued.

III. Privacy by Design

Reed Elsevier supports the concept of privacy by design. We always consider privacy when developing our products. The purpose for which a product is developed drives decisions made about its design, and privacy protections are a very important factor in this calculation. Information products are routinely evaluated on privacy and security grounds before determining which market segment(s) will be permitted access to the product. For example, a database that contains sensitive personal information such as social security numbers will be limited to the particular segments of the market that require that information. Even then, potential customers are subject to a strict credentialing process prior to such access being given. Products are also carefully reviewed to make sure that they comply with existing privacy regimes.

A. Business Need Requires Certain Types of Data Be Retained Indefinitely

Reed Elsevier is concerned about the data retention requirements proposed in the Report. The Report proposes that consumer data be retained for "only as long as they [companies] have a specific and legitimate business need to do so."[2] The concept of "specific and legitimate business need" requires further refinement, as a number of Reed Elsevier's research products include documents that are intended to be retained indefinitely, or for which the business need to retain information is ongoing. News reports, documents of historic significance, information with precedential value like court decisions, and official public records such as land title records, are examples of data that is retained without temporal limits. Their inclusion in our databases enhances the value of these databases and provides demonstrable public and societal benefits by providing

[2] Report, p. 46.

a complete historical record for researchers and members of the public. Indeed, the Commission itself in its Report cites to historical documents, including a 25-year-old legal precedent and a 120-year-old law review article,[3] neither of which would have been available had a retention limit of less than 25 years been applicable.

For many of our other products, the business need to retain information is ongoing. For example, with LexisNexis' authentication and fraud detection products, historical information about an individual is often useful to law enforcement officials who seek to draw connections between potential fraudsters who may share address or name information. In addition, for businesses that purchase their data from third parties, it is not always possible to know when data was initially collected. Imposing a retention requirement on many different types of data is simply not practical.

Distinctions between data-based products and business records can result in vastly divergent treatments. Decisions based upon business necessity and other considerations may drive significantly different results for similar data, *e.g.,* data collected from customer transactions may be retained for longer periods of time for active customers than for customers who no longer enter into new transactions. Similarly, the existence of an inquiry or investigation could disrupt normal data retention and destruction cycles. It is important that businesses should have the flexibility to make informed decisions about how long data should be retained.

B. Data Accuracy

For information companies like LexisNexis that collect data from third parties, we consider our data to be accurate if it mirrors the data we receive from reliable third party sources. We are concerned that the accuracy verification requirements proposed by the Report could result in new, unworkable requirements being imposed on companies like ours that collect data from reliable third party sources. For companies that procure data from reliable third party sources and not from consumers directly, verifying that the reported data matches the data provided by the consumer to the original recipient is not possible, since the company has no relationship with the consumer and has no control over how the data is sourced. Similarly, some data is subject to conflicting opinions on accuracy and correctness. Data sourced from a government agency or court includes a presumption of correctness notwithstanding conflicting claims from a consumer (absent documentary support that the issue has been specifically addressed by the agency or court). Attempting to verify data through other means would impose costly and inappropriate requirements on information companies and would have a negative effect on businesses that depend upon information from reliable third party sources.

A more narrow proposition to verify the accuracy of data against the third party source from which it was acquired, *i.e.*, to verify that the data was not inadvertently and substantively altered in any way post-acquisition, may be workable for some businesses, but this proposition must be carefully vetted to ensure that it can be successfully implemented without imposing an excessive burden on information companies.

---

[3] *See* Report nn. 1 & 178.

Data collected for specialized uses, such as the production of consumer reports under the FCRA, is subject to special rules with regard to accuracy. FCRA data is subject to additional safeguards, including limitations on acceptable sources. These safeguards raise the level of data accuracy as well as the cost. While the FCRA safeguards on data accuracy are appropriate for data used for decisions involving employment, credit, insurance, or housing, these same safeguards do not make sense for data used for other purposes For example, imposing FCRA-like correction requirements on information contained in printed telephone directories does not make sense as this information is not intended to be used to make critical decisions involving consumers, and updates more frequently than annually are cost prohibitive.

IV. Simplified Choice

Reed Elsevier supports the Commission in not requiring choice to be provided to consumers before collecting and using consumers' data for "commonly accepted practices." We commend the Commission for recognizing that businesses need not request consent to engage in fraud prevention activities, legal compliance, and other practices necessary for public policy reasons. Our comments below detail several specific examples of "commonly accepted practices." However, our comments are not exhaustive on this point as there are many instances where consumer expectations and business practices are consistent and where choice need not be required. The use of consumer information in order fulfillment is but one example. It is critical that the Commission approach this issue judiciously.

A. Fraud Prevention Exception

One of the commonly accepted practices called out in the Report is "fraud prevention," citing fraud detection services used by online businesses to prevent fraudulent transactions.[4] While we strongly support the inclusion of a "fraud prevention" exclusion, it is important that "fraud prevention," or the more general "commonly accepted practices" exclusion also include fraud detection, identity authentication and law enforcement applications. Identity authentication, *i.e.*, verifying that a person is who they claim to be, is essential to protecting consumers and preventing identity theft. Providing information needed to support law enforcement efforts and criminal investigations should also be excluded from the choice requirement.

Because LexisNexis data is used for law enforcement, public safety and anti-fraud purposes, providing criminals and fraudsters with the opportunity to opt-out of having their information included in our data would significantly diminish their effectiveness. Moreover, it is not workable for an information company that does not collect information directly from the consumer to implement a choice mechanism. It is unclear at what point choice could be provided, since information companies do not interact directly with consumers.

[4] Report, p. 54.

B. First Party Marketing

Reed Elsevier supports a broad definition of "first party marketing." First party marketing should include business affiliates and should not require choice. Reed Elsevier operates hundreds of websites under different names, but all are under the common control of Reed Elsevier. To require that these websites be segregated from one another for marketing purposes would be to impose a burden on Reed Elsevier without a corresponding benefit to the consumer, who after doing business with one website in the Reed Elsevier family of companies may be interested in receiving tailored offers from other related sites. Similarly, first party marketing should not require choice, irrespective of the channel in which the marketing occurs, whether email, postal mail or text messaging.

In addition, Reed Elsevier supports the inclusion of third party marketing as a commonly accepted practice for which choice is not required. Third party marketing is a very commonly accepted and used practice among commercial and non-profit entities. Both first party and third party marketing are extremely common practices that have occurred in some form for decades. Throughout this history, consumer choice has been construed to require allowing customers an opportunity to opt-out of unwarranted practices. Altering this status quo would drastically change the landscape of information flow and, in the online context, would disrupt the online experience as we know it. The data sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. At this time, these interactions are seamless and happen out of sight of the consumer. There is little to no harm to consumers by having their information included in a marketing database and adding a choice requirement for marketing would only serve to disrupt the consumer experience.

C. Do Not Track

Reed Elsevier is concerned that a Do Not Track mechanism could negatively impact the ability of companies to collect and use information from their customers to develop new products and enhance their existing products. A Do Not Track mechanism, if implemented broadly, could potentially prevent Reed Elsevier from collecting the site operational information it relies upon for billing and to assist in the development of new products and services. Moreover, the online advertising business is a highly dynamic market characterized by rapid technological change. In this environment, regulation that is specific to a technology or business model could deter entry, thwart innovation, and limit competition in the sale of online advertising, as well as limit the products and services that consumers are accustomed to receiving for little or no cost because they are sponsored by advertising.

While we support uniform choice for consumers for online behavioral advertising, we believe that the government should not get involved in the development of a Do Not Track mechanism. At this time, significant self-regulatory efforts are underway that will provide uniform consumer choice for online behavioral advertising, as contemplated by the Commission, without sacrificing potential innovation in new products and services.

These efforts are based on the Self-Regulatory Principles for Online Behavioral Advertising (the "Self-Regulatory Principles") released in July 2009.[5] The Self-Regulatory Principles include a consumer choice principle, which enables users of Web sites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred after reviewing information regarding the advertisements.

D. Business Contact Information

Use of business contact information obtained from a business card, letterhead, or signature block should also be clearly exempted from any choice requirements on the grounds that this is business information, not "consumer" information. Alternatively, use of business contact information should be permitted as a commonly accepted practice, the voluntary disclosure being presumed to constitute consent.

V. Greater Transparency

A. Access and Correction

As part of the movement towards greater transparency, the Commission proposes that companies should provide reasonable access with the right to correct the consumer data they maintain. We have serious concerns with the access and correction requirement outlined in the Report. As discussed above, many of our products are used for fraud detection and law enforcement purposes. Reed Elsevier is concerned that an access and correction requirement could be misused by criminals to gain access to databases in order to perpetrate fraud against consumers based on data obtained from those databases. No verification system can be made perfect. The imposition of an access obligation on databases that contain personal information can facilitate fraud and other criminal activity by allowing criminals to "game" the system. Criminals already exploit existing access rights to gather additional information for use in fraud schemes, such as "phishing" or other scams that use known information to induce consumers to reveal more compromising personal information.

Similarly, imposition of a correction requirement for data obtained from third parties, including data obtained from government agency records or from proprietary private sources such as journalistic reports and research articles, raises the possibility that consumers could seek changes to widely distributed versions of public records resulting in privately held versions that differ from the official records. Such a change could take the form of a change to the name of an owner on a property record or an alteration in the outcome of a court decision. Similarly, changes to news reports should be made only by the publisher and author, not by the distributor who did not create the content, notwithstanding the consumers' disagreement with the substance of the report.

No additional correction requirements should be proposed. Under the FCRA, consumers are already entitled to receive notices for the most impactful adverse actions

---

[5] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf.

that may result from the use of personal information, such as denials of employment, credit or insurance. Adverse action notices should not be expanded to include a vague concept like "denial of benefits." The FCRA also provides the affected consumer with the right to request a disclosure of the information that the consumer reporting agency maintains about him or her and that is used for the compilation of a consumer report. Applying a correction right more broadly than in the FCRA context would impose significant new compliance costs on a huge number of businesses with little or no additional benefit to consumers. There is also repeated evidence in the credit context of "credit repair" activities that seek to improperly "correct" credit histories. Creating that same risk by needlessly applying FCRA-like correction rights to vital non-FCRA services used to prevent fraud and catch criminals would hurt the public interest and increase the risks of identity theft.

For example, allowing a consumer to "correct" address information contained in a commercial database may impede criminal investigations or prevent law enforcement from locating a material witness in a child abduction case. Even a narrow correction requirement can have unintended consequences where the person requesting the correction uses this right to falsify the record. Reed Elsevier's data is used for multiple purposes, and allowing correction for one purpose, such as identity authentication, can diminish the value of the data when used for other purposes, such as fraud detection and prevention or law enforcement. It is critical that a correction mechanism not burden services' efforts to stop fraud and identity theft and that the business maintaining the data be able to reject a request that data be changed where the requester has not met reasonable standards for establishing the correctness of the requested change.

B. Express Affirmative Consent

The Report also calls for prominent disclosures and obtaining express affirmative consent before using consumer data in a materially different manner than claimed when the data was collected or obtained.[6] These provisions are unworkable for information companies and would severely undermine the effectiveness of our information products.

Reed Elsevier purchases data from reliable third parties; however, it would not be possible to provide notices and obtain affirmative consent from a sufficient number of individuals and maintain comprehensive information in our databases. Even if we could convince our data suppliers to provide disclosures and seek such affirmative consent, we know from historical experience that the numbers of individuals who respond to an opt-in request will be extremely low. Moreover, data we obtain from public records is public as a matter of law and does not require consent for data collection and use.

In addition to the practical difficulty of obtaining affirmative consent, many of the socially beneficial uses for data would be negatively impacted under the proposed regime. Data used to locate criminal suspects, monitor registered sex offenders, and enforce court judgments must be comprehensive to be of optimal value. Data used to detect and prevent fraud must also be all-encompassing. Requiring affirmative consent for inclusion of this data ensures that the data loses its effectiveness and utility as those

[6] Report, p. 76.

persons whose participation is most essential will also be the individuals least likely to consent.

C. Notice

The notice requirement included in the Report is not workable for companies like Reed Elsevier that do not collect information directly from individuals. It is unreasonable to require companies that have no customer relationship with individuals to provide notice to such individuals as suggested in the Report. Information companies like Reed Elsevier collect information from a variety of reliable third-party data sources. With the high volume of records we collect each year, providing notice and opt out options to each individual is not possible.

Reed Elsevier supports the ability for private industry to communicate a "take it or leave it" proposition to consumers via the privacy pledges contained on their websites, which would mandate that a consumer's use of a website, product or service constitutes consent to the company's information practices. As discussed above, affirmative consent from consumers can be difficult to obtain. Many consumers are likely to be generally comfortable with the information practices of their favorite websites and would most likely prefer to have their website use continue unimpeded. But for the other website users who are sensitive to particular information practices, the prominent display of a user-friendly website privacy policy, coupled with the user's ability to register his discomfort with the website's privacy practices by simply leaving the site, is a flexible solution that accommodates all manner of users and will provide valuable feedback to websites that wish to adopt privacy practices that maximize traffic to their website.

Private industry should have the flexibility to determine its information practices and present them to the public to allow the marketplace to decide what information practices it prefers. The Report asks for input into any circumstances where a "take it or leave it" proposition would be unacceptable. Websites that provide a public service and may be the single source for certain information, such as outsourced government agency websites, should not condition their use on the consumer's acceptance of information practices. The websites of private industry, however, should not be subject to the same constraints.

* * *

Reed Elsevier appreciates the opportunity to provide these comments to the Commission. We commend that Commission for its continued leadership in the area of consumer privacy and for providing various forums for stakeholders to provide input on the complex public policy issues involving consumer privacy. While Reed Elsevier supports the FTC's goal of protecting consumer privacy, we have concerns with some of the key components outlined in the proposed framework that are unworkable for non-consumer-facing companies.

It is important that any policy recommendations included in the final report recognize the important distinction between companies that collect information directly from consumers and those that do not. Any policy recommendations that attempt to uniformly apply the FIPPs across all businesses will significantly harm information

companies and hinder the ability of those companies to provide critical information to businesses and government agencies to detect and prevent fraud and for other important purposes, and ultimately have a negative impact on consumers.

We urge the Commission to consider carefully the impact that any proposed policy recommendations would have on information used for fraud detection, prevention, identity authentication and law enforcement purposes. Including an access and correction and opt out requirement for databases used for these important purposes would allow criminals and fraudsters to "game" the system and avoid detection. Finally, we urge that the Commission to remove the affirmative consent requirement as this requirement is unworkable for information companies and would severely undermine the effectiveness of our information products. We look forward to working with the Commission in addressing these important public policy issues. If you have any questions regarding these comments, please call me or contact Steve Emmert, Senior Director, Government & Industry Affairs, at (202) 857-8254.

Sincerely,

Steven Manzo
Vice President, Government Affairs
Reed Elsevier Inc.