

**ATTORNEY GENERAL'S LEGISLATIVE PROGRAM
PROGRAM BILL # 19-05**

Senate #

Assembly #

**Attorney General Eliot Spitzer
The Capitol, Albany, NY 12224
(518) 486-3000**

MEMORANDUM

AN ACT to amend the general business law and the executive law, in relation to protecting personal information collected and distributed by information brokers

PURPOSE:

This bill protects the privacy of confidential personal information by enabling individuals to prevent information brokers from disclosing such information to certain third parties.

SUMMARY OF PROVISIONS:

Section 1 of the bill states legislative findings.

Section 2 of the bill adds a new Article 32-A to the General Business Law, which sets forth certain protections relating to confidential personal information collected by information brokers.

New General Business Law § 676 defines certain terms, including the following:

“Confidential personal information” is defined as: (a) social security information; (b) mother’s former and current names; (c) birth date; (d) non-published telephone numbers; (e) records of telephone calls made and received; (f) income (g) bank account and investment information; (h) tax information; (i) organization memberships and donations; (j) purchasing information or preferences; (k) medical information; (l) driving record; (m) criminal record; or (n) history of civil actions.

“Information broker” is defined to mean an “individual reference services provider” or a “marketing list broker”. An “individual reference services provider” means any person or entity who engages in the business of providing reports containing confidential personal information about individuals to third parties for compensation. A “marketing list broker” means any person who, for compensation, provides reports containing names, mailing addresses or electronic mail addresses of individuals categorized by characteristics, conditions, circumstances, traits, preferences or mode of living.

The terms “information broker”, “individual reference services provider” and “marketing list

broker” do not include: (a) governmental entities, or persons providing information to governmental entities; (b) consumer reporting agencies providing consumer reports and investigative consumer reports, or persons furnishing information to consumer reporting agencies; (c) businesses sharing information with affiliates; (d) entities with an established business relationship with the data subject; (e) news organizations; (f) licensed private investigators when providing certain types of information; or (g) labor unions.

New General Business Law § 676-a authorizes individuals to determine that confidential personal information should be excluded from reports prepared by individual reference service providers (IRSPs). Every IRSP is required to establish a notification system (including a toll-free telephone number) through which an individual can provide notice that confidential personal information should be excluded. IRSPs are prohibited from disclosing confidential personal information after receipt of such notice, except that no penalties will be imposed for disclosures made within five business days after the notice if the IRSP proves that the data was disclosed in response to a request received prior to receipt of the election and IRSP took all reasonable steps to prevent disclosure.

Whenever an IRSP issues a report containing confidential personal information (except for reports issued to a government agency or pursuant to a court order), the IRSP will be required to send a written notice to the individual who is the subject of the report. This notice must provide the name and address of the individual or entity who requested the report, and must advise the data subject that he or she has a right to receive a copy of the report and to have confidential personal information excluded from future reports.

In addition, upon request of an individual, an IRSP is required to disclose the nature, contents and substance of all personal information in its file relating to the individual, and to provide the names and addresses of any recipients of reports about the individual provided within the prior 12 months (other than reports issued to government agencies or pursuant to court order). Finally, IRSPs are required to establish appropriate safeguards to ensure the security and confidentiality of their records.

New General Business Law § 676-b imposes requirements on marketing list brokers that are identical to the requirements imposed upon IRSPs, except that: (1) marketing list broker are not required to establish a formal notification system and a toll-free telephone number; and (2) marketing list brokers are not required to advise individuals when they have been included in a marketing report.

New General Business Law § 676-c requires the Secretary of State to establish and operate (or enter into an agreement with another entity to establish and operate) two exclusion lists: (1) an IRSP exclusion list consisting of the data subjects who do not want their confidential personal information disclosed; and (2) a marketing report exclusion list consisting of those subjects who do not want their marketing information released. Each data subject who has elected to opt-out shall remain on the list until the notification is rescinded. The lists shall be published at least quarterly in hard copy and may be available in other formats. IRSPs and marketing list brokers are prohibited

from issuing reports containing confidential personal information or marketing list information relating to any individuals on the exclusion list, but penalties may not be imposed for any disclosures with five business days after the a name first appears on the exclusion list.

In addition, the Secretary of State is required to promulgate rules governing the methods by which a data subject may give notice to be placed on the exclusion list, the procedure through which a data subject may revoke a notice, the methods by which any information broker may obtain access to the list, and the procedure for advising the public about the existence of the exclusion lists. The Secretary of State may impose a charge on information brokers in an amount calculated to defray the cost of operating the list. Moreover, information obtained in compiling the exclusion lists may be used only for compliance with this legislation, and shall not be subject to public inspection or disclosure.

New General Business Law § 676-d authorizes the Attorney General to bring enforcement actions for violations of new Article 32-A, including injunctions and civil penalties of not more than \$1,000 per violation. In addition, new General Business Law § 676-e provides a private right of action for any data subject whose confidential personal information is disclosed in violation of Article 32-A. The data subject can recover actual damages or \$1,000, whichever is greater, as well as reasonable attorney's fees, and may increase the damage award to \$5,000 for willful violations.

Section 3 of the bill adds a new Section 101 to the Executive Law, which contains a cross reference to Article 32-A of the General Business Law.

Section 4 of the bill contains a severability clause.

The bill takes effect 180 days after enactment.

EXISTING LAW:

There are no current prohibitions on the transfer of confidential personal information by information brokers. However, there are existing restrictions on the collection and use of personal data by government agencies and some types of businesses. For example, the Personal Privacy Protection Act (Public Officers Law, Article 6-A) imposes restrictions on the ability of certain state agencies to collect and disseminate personal information about New York residents. Agencies subject to the act must maintain only the personal information which is relevant and necessary to accomplish the purpose of the agency, must provide certain notifications when information is collected, and must provide individuals with access to records about them and an opportunity to correct or challenge the contents of the records. However, this act does not apply to private businesses.

Similarly, the Fair Credit Reporting Act (General Business Law §380-a *et seq.*) regulates the collection and use of personal data by credit reporting agencies. Specifically, the act provides as follows: 1) if a consumer report is used in any decision to deny credit, insurance, or employment,

the report user must tell the consumer the name and address of the reporting agency; (2) consumer reporting agencies are prohibited from disclosing consumer reports without consent, unless such disclosure is made for a legitimate business purpose or pursuant to a court order; (3) reporting agencies must institute procedures to avoid reporting specified categories of obsolete information and to verify information in investigative consumer reports that are used more than once; (4) consumer reporting agencies must maintain security procedures, including procedures to verify the identity and stated purposes of recipients of consumer reports; and (5) individuals may sue credit reporting agencies or parties who obtain consumer reports for violations of the Act, and may recover for actual damages suffered, as well as attorney's fees and court costs.

JUSTIFICATION:

Individuals in today's society must engage in a wide variety of commercial, financial and other transactions with local and national businesses, educational institutions and other organizations. These transactions frequently involve the transfer of information that is inherently private, which the individual would prefer not to reveal.

When engaging in these transactions, many individuals appropriately assume that the information being provided will be treated as confidential and will not be disseminated to others. The information generally is necessary solely to complete the transaction and to deliver the necessary goods or services, and further sale or dissemination of that personal private information to others is not a consequence anticipated or desired by the consumer.

Despite the strong interest that individuals have in preserving the confidentiality of this private information, details about their finances, habits, purchasing preferences and backgrounds are routinely sold or otherwise released for commercial or other purposes. Advances in information technology have facilitated the compilation, sophisticated analysis and wide dissemination of massive amounts of data, at ever decreasing costs, and this has enabled many entities to gain access to private personally identifiable information without the knowledge and consent of the person to whom the information relates.

As a result, consumer information has now become a marketable commodity, and businesses have been created for the sole purpose of collecting, analyzing and selling confidential personal information. In particular, two types of businesses have arisen: (1) "individual reference services providers" (IRSPs), which sell "profiles" and other reports containing confidential personal information about individuals; and (2) "marketing list brokers", which sell lists of names, mailing addresses or electronic mail addresses of individuals, grouped by characteristics, conditions, circumstances, traits, preferences or mode of living.

The activities of IRSPs and marketing list brokers have resulted in a dramatic proliferation of large electronic databases containing a wide array of data. The data ranges from purely identifying information (such as social security number, date of birth and mother's maiden name) to much more extensive details, including driving records, criminal and civil court records, licensing

records, investment and other financial information, association memberships, unlisted telephone numbers, air travel records and histories of purchase activity and telephone use.

When transactional data from different sources are collected in a single place, a detailed dossier of spending habits, lifestyle, associations, work practices, legal information, medical data and other information can be created. For example, a simple monthly billing statement, when combined with other databases provides a readily accessible list of all items purchased, when and where they were purchased and other lifestyle information. Virtually any purchase that an individual makes -- food, clothing, over-the-counter medications, hair dye, pregnancy test kits, alcohol, magazines, diet pills, etc. -- can be noted in these records. Thus, an unknown third party could learn more about an individual's lifestyle than the individual's closest friend.

Consumers are often unaware of the existence of these ever-growing profiles, or that confidential personal information is sold to a broad spectrum of commercial customers at low prices. Recently, there was a major breach of security at ChoicePoint, an information broker that maintains an estimated 19 billion items of information about millions of individuals. Personal data, such as names, current and former addresses, social security numbers and telephone numbers of unsuspecting individuals, who do not know their information was on file at ChoicePoint, is now in the hands of identity thieves.

Moreover, consumers may be adversely affected by the misuse of data, or the reliance on inaccurate information. For example, if the information provided in an application by a consumer does not match the information obtained from an information broker or an individual reference service provider, the consumer may be denied credit, employment or other opportunities. Given the ease in which this information is accumulated, aggregated and shared, errors can be replicated and the harm long-lasting, mismatched data could result from records compiled from several sources.

The easy availability of key identifiers may also lead to increased incidence of identity fraud. Identity fraud involves financial exposure of victims and financial institutions, and it can take many years for individuals to clear their reputations and re-establish their own identities and records. The dissemination of confidential personal information also creates other risks, including: (1) potential physical harm perpetrated by stalkers and other abusers gaining access to information from vendors; (2) the proliferation of fraudulent, misleading, intrusive and deceptive telephone, direct mail and Internet solicitations; and (3) undue embarrassment for individuals who have had private information revealed without their consent.

This bill seeks to address these problems by imposing restrictions on the ability of information brokers to disseminate confidential personal information about individuals. Specifically, this bill authorizes New York residents to protect their personal data by having their names placed on an "exclusion list" maintained by the Secretary of State, or they can advise an information broker directly that they want their confidential information protected. IRSPs and marketing list brokers will then be prohibited from disclosing confidential personal information or marketing information about any individual included on the Secretary of State's exclusion list or who has otherwise indicated that they want this information protected. In addition, whenever an

IRSP issues a report containing confidential personal information (except for reports issued to a government agency or pursuant to a court order), the IRSP will be required to notify the individual who is the subject of the report.

The bill also provides that, upon request of an individual, every information broker will be required to disclose the nature, contents and substance of all personal information in its file relating to the individual, and to provide the names and addresses of any recipients of reports about the individual provided within the 12 month period (other than reports issued to government agencies or pursuant to court order). Information brokers will also be required to establish appropriate safeguards to ensure the security and confidentiality of their records.

The bill authorizes the Attorney General to bring enforcement actions for violations of these restrictions, including injunctions and civil penalties of not more than \$1,000 per violation. In addition, any individual whose confidential personal information is disclosed illegally will be able to bring an action and recover actual damages or \$1,000, whichever is greater, as well as reasonable attorney's fees, and damages up to \$5,000 if the violation is willful.

Technology is advancing at a pace never before seen in our history, and although there are many benefits, government should act to ensure that the public's fundamental right to privacy is not be inappropriately abridged.

PRIOR LEGISLATIVE HISTORY:

This bill was introduced as S. 5011/A. 8031 during the 2003-04 legislative session, and S.5239/A.8332-A during the 2001-02 legislative session.

FISCAL IMPLICATIONS:

There are no fiscal implications.

EFFECTIVE DATE:

The bill takes effect 180 days following enactment.