Report to the General Assembly of the Data Broker Working Group issued pursuant to Act 66 of 2017

December 15, 2017

Issued by
Office of the Attorney General
Department of Financial Regulation

Table of Contents

I. Preamble 1

II. Executive Summary 1

III. Background 3

A. Legislative Mandate and the Working Group's Process 3

B. The Data Broker Industry is an Important and Growing Component of the Economy 3

C. The Equifax Breach Highlighted both the Risks of Data Aggregation and the Extent of Public Concern Associated with it 5

D. Benefits of the Data Broker Industry 6

E. There are Significant Risks Associated with the Widespread Aggregation and Sale of Data about Individuals by Data Brokers 7

F. Security Breaches 10

G. Past investigations into the Data Broker Industry 12

IV. Current Regulatory and Legal Background 13

A. Federal Protection of Consumers 13

B. State Protection of Consumers 14

C. Areas Subject to Both State and Federal Regulation 15

D. State Laws Without Direct Federal Counterparts 17

E. Federal Laws Without Direct State Counterparts: 18

F. The European Regulatory Regime: 20

G. Proposed legislation at the federal level or in other states 22

V. Recommendations 23

A. Definition of "Data Broker" 23

B. Regulation of Data Brokers 24

1. Credit Freeze Fee 25

2. Increase Consumer Awareness of Data Broker Opt-Out Rights 25

3. Prohibit Acquisition of Data for Illegal Purposes 26

4. Minimum Data Security 27

5. Swift Notice of Security Breaches 28

6. Protecting Children 29

Bibliography 30

Exhibit A: Stakeholder Recommendations i

Exhibit B: Massachusetts Data Security Regulation vi

I. Preamble

Information collection in commerce benefits consumers and industry. The bargain is that consumers provide information in exchange for transactional ease. Industry, on the other hand, not only acquires and possesses that information, in some cases, it transforms and commodifies the information. As a result, industry may facilitate not just the initial consumer transaction, but other transactions as well. This may lead to additional economic activity, but it also may pose risks to consumers who are unaware of secondary transactions involving the information they provide.

Data Brokers are businesses that collect personal data in order to resell it to third-parties. Vermont's citizens and the General Assembly have expressed concerns about practices within the Data Broker industry and possible harms that could arise from their activities. This report proposes for the Legislature's consideration several potential responses to these concerns, while also recognizing the importance of commercial transactions in the information economy.

II. Executive Summary

The Working Group convened under Act 66 of 2017 — comprising the Attorney General's Office and the Department of Financial Regulation — has studied the data-broker industry, heard extensive testimony in public meetings, and received written comments. It makes the following recommendations to the General Assembly for legislation that would protect Vermonters — particularly Vermont's most vulnerable — from the potential harms posed by the widespread storage and sale of sensitive data.

The Working Group, in making these recommendations, recognizes that the Data Broker industry includes many reputable companies that are crucial to the modern economy and are already making many efforts to protect consumers' data and privacy. The recommendations seek to impose minimal burdens on the industry as a whole, while also fulfilling state government's vital, longstanding role in protecting consumers.

The Working Group recommends the following definition of "Data Broker":

> A commercial entity that (1) assembles, collects, stores, or maintains personal information concerning individuals who are not customers or employees of that entity, and (2) sells the information to third parties.

Several types of businesses are not included in this definition. They are set forth in § V.A. The Assembly may decide to make these exemptions explicit.

The Working Group also recommends for consideration by the Legislature the following six potential actions that balance the benefits of the Data Broker industry with the potential harms of certain practices:

1) Amend Vermont's credit-freeze law (9 V.S.A. § 2480h) to prohibit credit reporting agencies from charging a fee to freeze or unfreeze consumers' credit reports;
2) Provide consumers with more information about opt-out rights and how to exercise them, by requiring Data Brokers to provide the Secretary of State with certain information;
3) Create new causes of action, enforceable by a consumer or the Attorney General, against those who acquire data with the intent of committing certain wrongful acts;
4) Require Data Brokers to employ reasonable security methods to protect data;[1]
5) Require Data Brokers that suffer certain data breaches to quickly provide notice of the breach; and
6) Protect children by prohibiting the sale of data about certain minors without parental consent.

While further legal analysis and discussion is required, the Working Group's preliminary research and legal analysis indicates that the litigation risk involved in the first three considerations is relatively low. The latter three may involve more substantial risks that the Assembly will want to carefully consider, in consultation with legislative counsel, DFR, and the AGO, in determining whether the potential benefits to the public outweigh the risks to the State.

[1] Note that Massachusetts has a data-security statute that applies to all businesses and is not limited to data brokers.

III. Background

A. Legislative Mandate and the Working Group's Process

In Act 66, the Vermont General Assembly directed the Attorney General's Office ("AGO") and the Department of Financial Regulation ("DFR") to study the data broker industry and potential regulation.[2] Specifically, the General Assembly asked the Working Group to submit a recommendation or draft legislation by December 15, 2017 that reflects (A) an appropriate definition of the term "data broker"; (B) whether and, if so, to what extent the Data Broker industry should be regulated by either DFR or the Attorney General; (C) additional consumer protections; and (D) proposed courses of actions that balance the industry's benefits with its actual and potential harms.[3]

Beginning in June 2017, DFR and AGO representatives formed a Working Group that met, studied the issue, and discussed potential regulatory solutions. The Working Group agreed that it was important to hear from all interested stakeholders before reaching any conclusions in the study.

The Working Group convened two days of public hearings in Burlington on July 25 and 26, 2017.[4] Representatives of industry trade groups, national Data Brokers, and local business[5] appeared and offered testimony, as did local, national, and international consumer and privacy advocates.[6] The Working Group also solicited and received written comments, and had several informal conversations with stakeholders.

B. The Data Broker Industry is an Important and Growing Component of the Economy

The Data Broker industry, generally speaking, is the group of businesses engaged in the acquisition, aggregation, analysis, and sale of information about individual consumers. The industry is, by a conservative estimate, a multibillion-dollar segment of the American economy, and growing.[7]

---

[2] 2017 Vt. Acts & Resolves No. 66, § 2. Copies of all documents referenced in this report have been stored in the Data Broker Working Group Document Repository, located at http://www.ago.vermont.gov/news-and-updates/data-broker-working-group1/data-broker-working-group-documents-referenced.php.

[3] *Id*.

[4] Video recordings of those hearings are available on the Attorney General's website, *at* http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php

[5] Among those who testified were representatives from Acxiom, the Consumer Data Industry Association (CDIA), CompTIA, the Data and Marketing Association (DMA), MyWebGrocer, RELX (formerly Reed Elsevier, which owns LexisNexis), and TechNet.

[6] Among those who testified were representatives from Amnesty International, the Vermont Network Against Domestic & Sexual Violence, VT PIRG, and the World Privacy Forum, and a professor from Fordham University School of Law.

[7] *See* Senate Comm. On Commerce, Science & Transp., Staff Rep. for Chairman Rockefeller, Executive Summary, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Dec. 18, 2013.

The Industry, by its nature, operates on a national scale, and has grown significantly in past decades due to advances in technology, including the internet and smart phones, increases in processing power, and decreases in data storage costs.

"Data Broker" or "Data Aggregator" is a broad term for a commercial entity whose primary line of business is the acquisition, aggregation, analysis, and resale of personal data. Data Brokers acquire a broad variety of information from a wide range of sources. For example, Data Brokers commonly gather data from: internet browsing history; online purchases; publicly available information (such as information maintained by state or local governments like property records, motor vehicle records, or court cases, or otherwise accessible information like social media connections and posts); location data; and registration or subscription information (such as magazine subscriptions or loyalty-card data from a grocery store). Data brokers also obtain information from federal and state government entities, by purchasing it from the source of the data (for example, from a social media website or blog, or from a brick and mortar store), and from other Data Brokers.

Data Brokers often combine data from several sources, allowing them to create extensive dossiers of information on individuals, sometimes including thousands of data points on a single person. Some Data Brokers focus primarily on collecting raw data from multiple sources, combining it, and "cleaning up" the data (i.e. confirming its accuracy). These data sets are then sold for use to various businesses.

Some Data Brokers also offer predictive analytics. Essentially, the Data Brokers apply algorithms to individuals' data based on correlations in data, and attempt to draw conclusions about consumers from their data. For example, based on the person's purchase history, online searches, social media "likes," and/or other inputs, a Data Broker might be able to extrapolate information about the individual's level of interest in a service or product, the individual's likelihood to purchase, physical or mental health, financial status, gullibility, tolerance for risk, addictions, or other likely attributes. The Data Broker can then add these conclusions to the data set and sell them as well. Consumer advocates have taken issue with the accuracy of these conclusions.[8]

Data Brokers sell information that is used for myriad business, government, and personal uses. The more prominent uses of information from Data Brokers include:

1) Targeted Marketing and Sales
    a) Mailing lists
    b) Telemarketing call lists
    c) Sales Staff Lead Generation
2) Targeted Online Advertising
3) Credit Reporting
4) Background Checks

[8] World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*, April 2, 2014 ("Scoring of America").

5) Governmental Investigations
6) Risk Mitigation and Fraud Detection – confirming that individuals are who they say they are
7) People Search
8) Rate Setting by banks, insurers, or others that may require extensive information about a customer
9) Decisions by banks, insurers, or others as to whether to provide services
10) Ancestry Research
11) Voter Targeting and Strategy by political campaigns

Some Data Brokers target customer bases in certain industries. For example, a company might acquire data from a large Data Aggregator, and repackage that data and sell mailing lists to marketers. A Data Broker may sell specific products to law enforcement or to financial institutions for public protection or regulatory compliance purposes. Other Data Brokers might offer data products, such as People Search or Ancestry Research services, via a website or app for general usage.

C. The Equifax Breach Highlighted both the Risks of Data Aggregation and the Extent of Public Concern Associated with it

On September 7, 2017, Equifax Inc. announced that it experienced a security breach involving the information of 143 million U.S. Consumers (the number was subsequently updated to 145.5 million) ("2017 Equifax breach"). Equifax is one of the three major U.S. credit reporting agencies. The breach exposed the personal information of 247,607 Vermonters (roughly 40% of the state's population). The acquired data included names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, the breach exposed approximately 209,000 credit card numbers and dispute-related documents with information for approximately 182,000 U.S. consumers.

In the weekend immediately following the breach, Vermont's Consumer Assistance Program ("CAP") received over 700 complaints, the highest volume of complaints it has ever received relating to a single incident. The Working Group also heard numerous reports of citizens contacting their legislators, and several newspaper articles and opinion pieces were written about the incident.[9] The breach has prompted action by several Vermont legislators, including a well-attended November listening tour of the state by members of the Vermont Legislature, members of the Executive Branch, and others. The listening tour held public hearings in Springfield and Barton on Nov. 9, 2017; and Manchester Center and Burlington on Nov. 14, 2017.

[9] *E.g.* Manjoo, Farhad, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. Times, Sept. 8, 2017,https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html; Andriotis, AnnaMaria et al., *Senators Rip Credit-Reporting Model in Wake of Equifax Breach*, Wall St. J., Oct. 4, 2017, https://www.wsj.com/articles/senators-rip-credit-reporting-model-in-wake-of-equifax-breach-1507136171.

Vermont consumers primarily criticized Equifax for its lack of reasonable data security, delay in reporting the breach, and issues in responding to consumer concerns (including crashed websites, insufficient call center support, an initial attempt to force consumers to waive their right to trial in favor of arbitration, and a mistaken instruction that sent consumers to a fraudulent website). Another common criticism was that Equifax was collecting this data at all, and that consumers had no control over the data collection.

In addition to credit reporting, which is regulated by FCRA and FACTA, Equifax also engages in Data Broker activity that is not within the scope of those federal regulations. The breach came three months into the Working Group's study, after the hearings. The breach itself, and the media and citizen response to it, highlighted issues for the Working Group to consider, including:

- Public concern about third-party collection of personal data is far higher than it appeared to be prior to the breach;[10]
- Equifax's notification time after it first learned of the potential breach has received significant criticism, indicating that at least for certain types of breach, a more rapid response is expected;[11] and
- Despite public representations to the contrary,[12] some large, sophisticated data brokers have not implemented reasonable data security to protect consumer information.[13]

The Working Group also participated in the listening tour and has taken these observations into account when making its recommendations.

D. Benefits of the Data Broker Industry

The Data Broker Industry provides critical services to the modern economy. Consumer data collected and sold by Data Brokers is used for various purposes, including risk mitigation, marketing, and people search products.

Risk mitigation includes background checks used by law enforcement, potential employers, and landlords. It also includes fraud detection services used by businesses, like banks, that must verify the identity of the person with whom they are doing business.

Marketing products are used to connect businesses with potential customers. This includes traditional services like selling mailing lists to direct mail or door-to-door marketers, phone lists

[10] In addition to the complaint volume received by CAP, Attorney General T.J. Donovan reports that the Equifax breach is the most common issue he was asked about in the fall of 2017 when meeting with constituents.
[11] Vermont's Security Breach Notice Act requires notice of a breach "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification . . ." 9 V.S.A. § 2435(b)(1).
[12] Stacy Cowley and Tara Bernard, *As Equifax Amassed Ever More Data, Safety was a Sales Pitch*, N.Y. Times, Sept. 23, 2017, https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html.
[13] This observation is supported by data breaches involving other data brokers, which are explained in more detail in Section III.F.

to telemarketers, and lead generation to sales forces. These products are also used to send marketing emails and to serve up targeted advertisements on websites.

This final use is particularly important, because many "free" websites rely heavily on revenues derived from targeted advertising. The Working Group heard testimony during the public hearings that without targeted advertising and the revenues it provides, the "free internet" as we know it would cease to exist.

People search products have essentially replaced the traditional phone book as a way of locating individuals, but in a far more broad-based and global manner. People search can be used to research corporate executives and competitors, to find old acquaintances, to research one's family history and to find other information. People search products can offer much more information than available in the phone book, including the names of relatives, criminal background, interests/hobbies, and other information.

E. There are Significant Risks Associated with the Widespread Aggregation and Sale of Data about Individuals by Data Brokers

Generally, Data Broker activity poses risk of two types of harm to consumers: (i) those related to consumers' ability to know and control the data collected and sold about them, and (ii) those that arise from unauthorized access to consumers' information. Although other potential harms exist, it would be impractical to create legislation that would address every conceivable harm created by the free flow of data about individuals.[14]

Consumers' ability to know and control their data is important in large part because inaccuracies are widespread. In 2012 the FTC reported that 21% of consumers sampled had discovered a "confirmed material error" in one of the credit reports issued by the three major credit reporting bureaus, and 5.2% of consumers had successfully challenged a mistake that was serious enough to lower their credit score and burden them with higher interest rates. A person's data profile can become corrupted either by a bad actor or by mistake. Given the complexity of data collection, such mistakes are commonplace and, once made, can propagate as the erroneous data is sold and resold. This was a critical issue that state and federal governments tried to address with the first Fair Credit Reporting Acts, which allowed

[14] For example, the Working Group heard testimony regarding the general impact on human rights that arises from a loss of personal privacy, such as a tendency to self-censor when one is unsure who is listening, or the impact on human dignity that comes of knowing that strangers are being given insights into one's mental health, private predilections, or secret purchases. *See also e.g.*, United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, June 30, 2014.

Another, more concrete harm comes from the discrimination that consumers may experience, generally without knowing, when businesses acquire legally sold data sets that are supposed to be used for marketing, and use them for eligibility purposes that can lead to discriminatory pricing, redlining, or refusing opportunities. For example, a university might deny admission to an applicant based on an analytic score that is primarily derived from shopping patterns. *Scoring of America*. Not all Data Brokers permit this use, however, and industry representatives testified that they prohibit the use of marketing data for eligibility purposes.

consumers to inspect and correct their own data. These credit reports are the one subset of the Data Broker industry that is currently regulated by FCRA and FACTA.[15]

For data not regulated under FCRA, if a consumer is placed on an irrelevant mailing list or has other material mistakes in his or her profile, or a business is inspecting a consumer's profile to make pricing or employment decisions, such negative actions do not have to be reported to the consumer. As FTC Commissioner (and former Vermont Assistant Attorney General) Julie Brill explained, "If data broker profiles are based on inaccurate information or inappropriate classifications, or used for inappropriate purposes, the profiles have the ability to not only rob us of our good name, but also to lead to lost economic opportunities, higher costs, and other significant harm."[16] For example, a consumer might be refused the ability to obtain mobile phone services based on erroneous data in a profile. The consumer might have no idea why the transaction was blocked if the decision was based on non-FCRA data.[17]

Targeting Vulnerable Populations

Data Brokers frequently sell lists that group individuals by common characteristics. Some Data Brokers sell lists of individuals who may be at heightened risk of harm. While industry representatives have argued that there are legitimate marketing or other purposes for these lists, such lists can expose consumers to targeting by unscrupulous marketers and worse (e.g. stalkers, harassers, perpetrators of frauds). Data brokers have sold the following lists:[18]

- Rape survivors
- Addresses of Domestic Violence Shelters (which keep their locations secret under law)
- Police Officers' and State Troopers' home addresses
- Genetic Disease sufferers
- Senior citizens suffering from dementia
- HIV/AIDS sufferers
- People with addictive behaviors, and alcohol, gambling, and drug addictions
- People with diseases and prescriptions taken (including cancer and mental illness)
- Consumers who might want payday loans, including targeted minority groups
- People with low consumer credit scores

Stalking and Harassing

Information obtained from data brokers may make it easier for a stalker or harasser to locate an individual and keep tabs on their activity. Of particular concern here are certain new harms

[15] FTC, *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003*, Dec. 2012.
[16] FTC, *Data Brokers, A Call for Transparency and Accountability*, Appendix C: Concurring Statement of Commissioner Julie Brill, May 27, 2014. ("FTC 2014 Report").
[17] *Id.*
[18] World Privacy Forum, *Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?*, Dec. 18, 2013.

enabled by the ease of obtaining and spreading digital information, for example: *doxing* (publishing someone's contact information online so they can be harassed by others), and *swatting* (calling in a threat to have a SWAT team descend on a person's house).[19] While these or similar methods have been possible on a local level for years using phone books and other resources, the internet has made them far more prevalent and simultaneously far more harmful, due to the sheer number of people who can potentially perform them.

The National Network to End Domestic Violence provides guidance on how survivors can remove themselves from some Data Broker lists.[20] The Vermont Secretary of State maintains the "Safe at Home" program,[21] which allows victims of domestic violence, sexual assault, and stalking to obtain a substitute address to avoid being found. As of early 2017 the Vermont program had 138 participants.

The Working Group heard testimony from advocates as to the difficulty or impossibility of completely removing oneself from Data Broker lists. While some Data Brokers permit individuals to opt out of their databases, consumers often have no way to know whether they are in a specific database, or how to opt out. And, some Data Brokers do not allow opt-out at all.

Identity Theft, Scams and Fraud

Information obtained from a Data Broker also may make it easier for a bad actor to engage in identity theft or other forms of fraud because of the accessibility and comprehensiveness of information regarding an individual. Identity theft can harm the individual whose life is thrown into disarray, but also the businesses whom the ID Thief subsequently defrauds.

A few examples of such misuse of information acquired from data brokers:

- In 2013, it came to light that US Court Ventures, a Data Broker, had been selling data to an identity thief who then resold that data to other identity thieves on the dark web. During part of the period when this was happening, US Court Ventures was owned by Experian.[22]
- In 2016, the FTC settled a case with a Data Broker called Leap Lab that bought hundreds of thousands of payday loan applications containing Social Security and bank account

[19] Geoffrey A. Fowler, *Your Data is Way More Exposed than You Realize*, Wall St. J., May 24, 2017, https://www.wsj.com/articles/your-data-is-way-more-exposed-than-you-realize-1495657390; *see also* Anna North, *When a SWAT Team Comes to Your House*, N.Y. Times, Jul. 6, 2017, https://www.nytimes.com/2017/07/06/opinion/swatting-fbi.html;.

[20] Nat'l Network to End Domestic Violence, *People Searches and Data Brokers,* 2013, https://nnedv.org/mdocs-posts/people-searches-data-brokers/.

[21] https://www.sec.state.vt.us/safe-at-home.aspx.

[22] Brian Krebs, *Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records*, KrebsOnSecurity, Mar. 10, 2014, https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/. *See also* Transcript of Waiver of Indictment and Plea to Information Hearing, U.S. v. Hieu Minh Ngo, Docket No. 1:12-cr-00144 Doc. 27, Mar. 7, 2014.

numbers, and then knowingly resold them to scammers, who emptied the accounts of millions of dollars.[23]

- The same year, the FTC obtained a default judgment against Sequoia One, LLC, another Data Broker that engaged in the same behavior.[24]
- Data Broker Information may be used for frauds other than identity theft. Information obtained from Epsilon in 2011, for example, was used in online fraud and spear-phishing attacks. (See Sec. III.F., below)

F. Security Breaches

Data brokers are a prime target for security breaches because they hold such large amounts of sensitive personal data aggregated in one place. The business community in general is subject to near-constant hacking attempts, and the Data Broker industry is no different. Even with reasonable security measures in place, some data breaches are inevitable. Accordingly, Vermont is one of 49 states with a Security Breach Notice Act, which requires businesses to notify consumers and the AGO or DFR when certain security breaches occur.[25] However, the type of acquired information that triggers the Act is very narrow, and information obtained in a breach of a Data Broker's site may not meet the requirements of the Act and may therefore be unreported. This leaves consumers vulnerable because they have not been informed that their information has been stolen.

For example, as discussed below, a breach involving usernames and passwords does not fall within Vermont's Act. A breach involving sensitive financial information or health information would not fall into the act if certain triggering data elements were not present. Finally, many Data Brokers claim to "aggregate, "anonymize," or "deidentify" data – in other words they store the data without a name, and therefore a breach including all of the data elements, but not the name, would not fall within the Act. The Working Group heard testimony that some Data Brokers may avoid storing information as PII, potentially limiting the efficacy of Vermont's

---

[23] Press Release, F.T.C., *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers*, Feb. 18, 2016, www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

[24] Press Release, F.T.C., *FTC Puts An End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts*, Nov. 30, 2016, www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

[25] 9 V.S.A. § 2435. The Act only requires notice when the breached data includes "Personally Identifiable Information," defined in 9 V.S.A. § 2430(5) as an individual's first name or first initial and last name in combination with a:

(i) Social Security number;
(ii) motor vehicle operator's license number or nondriver identification card number;
(iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or
(iv) account passwords or personal identification numbers or other access codes for a financial account.

Notice Act with respect to Data Brokers. Moreover, numerous studies have shown that such data can easily be re-identified with an individual based on as few as three data elements.[26]

In addition to Equifax, a number of other large data brokers have experienced data breaches. These breaches involved sensitive information but were not subject to Vermont's Notice Act because they did not involve PII as defined in the Act. Published accounts of alleged data breaches are increasingly common:

- Acxiom, one of the largest Data Brokers, was hacked in 2003, and over a two-year period over 1.6 billion records were stolen, including names, addresses, and email addresses, some of which were sold to spammers.[27]

- Epsilon, a Data Broker that held email marketing lists for thousands of clients, experienced a breach in 2011 which exposed the name and email addresses of millions of individuals. The breached emails were used for spam, email fraud, and "spear-phishing," targeted email attempts to obtain user credentials.[28]

- RELX, the parent company of LexisNexis, has experienced multiple breaches, including one in 2005 in which the Social Security numbers, driver's license information, and address of 310,000 people may have been stolen,[29] one in 2009 involving 32,000 individuals,[30] and potentially one in 2013 in which millions of records were stolen and potentially resold on the Dark Web.[31] The last breach also allegedly involved thefts from Dun & Bradstreet and Kroll Background America.[32]

- Experian discovered a breach in 2015 involving 15 million records that belonged to T-Mobile but were stored on Experian's servers. The records were accessed over a 2-year

---

[26] L. Sweeney, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf; Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous' People,* N.Y. Times*.,* Jan. 29, 2015, https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

[27] John Leyden, *Acxiom Database Hacker Jailed for 8 Years*, The Register, Feb. 23, 2006, https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/. Vermont's Security Breach Notice Act did not take effect until 2005.

[28] Miguel Helft, *After Breach, Companies Warn of E-Mail Fraud*, N.Y. Times, Apr. 4, 2011, https://www.nytimes.com/2011/04/05/business/05hack.html; Brian Krebs, *Feds Indict Three in 2011 Epsilon Hack*, KrebsOnSecurity, Mar. 15, 2006, https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/.

[29] Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. Times. *,* Apr. 13, 2005, https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html.

[30] Angela Moscaritolo, *LexisNexis admits to another major data breach*, SC Magazine, May 4, 2009, https://www.scmagazine.com/lexisnexis-admits-to-another-major-data-breach/article/555843/.

[31] Juan Carlos Rodriguez, *LexisNexis Could Have Suffered Data Breach, FBI Says*, Law360., Sept. 26, 2013, https://www.law360.com/articles/475918/lexisnexis-could-have-suffered-data-breach-fbi-says; Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KrebsOnSecurity, Sep. 25, 2013, https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

[32] *Id*.

period and came from consumer applications for device financing and other services, and contained names, addresses, Social Security numbers, dates of birth, and additional information.[33]

Current law does not fully account for the modern reality of Data Brokers holding tremendous amounts of sensitive — but non-PII — data, or for the increasing number of breaches of that data.

G. Past investigations into the Data Broker Industry

Because the Data Broker Industry is largely opaque, much of the information we have about it comes from investigations by federal government entities or consumer organizations, and subsequently issued reports.[34] These reports have aided our analysis and can be found in the Document Repository.

For example:

In December 2013, the U.S. Senate Committee on Commerce, Science and Transportation released *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, under the direction of then-committee Chairman Senator John Rockefeller.

In April 2014, the World Privacy Forum, a non-profit public interest research and consumer education group, issued *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*.

In May 2014, the Federal Trade Commission issued *Data Brokers: A Call for Transparency and Accountability*. This report was the result of a four-year study that began with the issuance of Orders to File Special Reports to nine data brokers pursuant to Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), and included follow-up communications and meetings.

Also in May 2014, the Executive Office of the President, President's Council of Advisors on Science and Technology issued *Big Data and Privacy: A Technological Perspective*.

In May 2016, the Executive Office of the President issued *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*.

[33] Notice was provided for this breach, as it fell within the definition of Vermont's Notice Act.

[34] FTC 2014 Report, at i ("The Commission noted that, while the FCRA addresses a number of critical transparency issues associated with companies that sell data for credit, employment, and insurance purposes, data brokers within the other two categories remain opaque.").

IV. Current Regulatory and Legal Background

The following are the primary laws governing this area:[35]

- Federal Laws with no State Counterpart:
    - Fair and Accurate Credit Transactions Act (FACTA) is an amendment to FCRA that was added, primarily, to protect consumers from identity theft;
    - The Do Not Call List, implemented by the FTC's Telemarketing Sales Rule, allows consumers to opt out of receiving certain telemarketing calls;
    - The Health Insurance Portability & Accountability Act of 1996 (HIPAA) applies to health care providers and their business partners;
    - The Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA) applies to financial institutions;
    - The Family Educational Rights and Privacy Act (FERPA) protects certain student information and applies to schools that receive federal funds;
    - The Children's Online Privacy Protection Act of 1998 (COPPA) applies to websites and mobile apps directed at children under 13; and
    - The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 gives guidance on what commercial email should include, and requires opportunities to opt out.
- State Laws with no Federal Counterpart:
    - Security Breach Notice Acts require notice to be given to consumers, and in some cases Attorneys General or other government actors, when a security breach occurs;
    - Social Security Number Protection Acts;
    - Safe Destruction of Documents Acts;
- Laws with State and Federal Counterparts:
    - Unfair and Deceptive Acts and Practices (UDAP) laws, including the Federal Trade Commission Act (and Vermont's Consumer Protection Act), are catch-all provisions that apply to a broad array of consumer protection issues;
    - The Fair Credit Reporting Act of 1970 (FCRA) applies to credit bureaus and those who provide information for, or use, credit reports;

A. Federal Protection of Consumers

The federal government has a number of privacy-related regulations, as described above, but they tend to be subject matter specific or "sectoral" – i.e., they regulate specific industries or activities. There is no single federal overarching privacy law. Because Data Brokers' activities tend to cut across sectors, they may be subject to an incomplete patchwork of regulation.

[35] As the Legislature is aware, in the fall of 2017, Legislative Council performed a comprehensive review of data-privacy regulation in general (i.e. not limited to data brokers) this fall. That review addressed some statutes and regulations that are beyond the scope of this report. The Review is available via the House Commerce & Economic Development Committee's website.

B. State Protection of Consumers

The State of Vermont has a long history of protecting its citizenry in the marketplace. The Consumer Protection Act (formerly called the Consumer Fraud Act, also sometimes called a "mini-FTC Act"), was enacted 50 years ago, in 1967.[36] Vermont's Fair Credit Reporting Act (or "mini-FCRA") was enacted in 1991.[37]

There are federal versions of these consumer protection laws. Specifically, Section 5 of the FTC Act (the "FTCA") parallels the Consumer Protection Act, and the Fair Credit Reporting Act is similar to Vermont's law. However, the FTCA does not preempt the CPA, and FCRA does not preempt Vermont's law. In fact, the federal FCRA contains express exclusions specific to Vermont's law.[38] Similarly, the Dodd–Frank Wall Street Reform and Consumer Protection Act,[39] which created the Consumer Financial Protection Bureau ("CFPB"), does not preempt the states' ability to regulate in the financial consumer protection area. Consequently, the states and federal government have long shared responsibility for regulating in this area, and frequently cooperate in enforcement actions.

The regulation of businesses that collect sensitive consumer data has also long been a domain of the states. The first Data Breach Notice Act was enacted in California in 2003.[40] Subsequently 48 other states and the District of Columbia adopted similar laws.[41] Vermont's Act was enacted in 2005. That same year, the General Assembly enacted laws regulating the use of Social Security numbers[42] and the safe destruction of documents containing personal information.[43] These laws are all housed in Chapter 62 of Title 9: Protection of Personal Information.

Chapter 62 is not limited to specific industries. There are no equivalent laws at the federal level.[44] Though, for example, data breach notification acts have been introduced in the U.S. Congress, the federal government has historically left regulation in this area to the States. There is no federal law that specifically regulates data brokers.

The areas where the US Government does address the collection and storage of sensitive information typically share enforcement authority with the States. For example, HIPAA

---

[36] 9 V.S.A. § 2453.
[37] 9 V.S.A. § 2480a.
[38] 15 U.S.C. § 1681t(b)(2).
[39] Enacted in 12 U.S. Code § 5491.
[40] California Civ. Code § 1798.82.
[41] A complete list of state data breach laws can be found at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] 9 V.S.A. § 2440.
[43] 9 V.S.A. § 2445.
[44] Federal laws address specific industries like health care (HIPAA), education (FERPA), and finance (GLBA), but there is no law of general applicability that addresses data breach, use of Social Security numbers, or safe destruction of information.

authorizes enforcement by state Attorneys General.[45] Graham-Leach-Bliley permits state laws that are not inconsistent, including state laws that offer greater protections than GLBA.[46]

In conclusion, regulation of Data Brokers is consistent with the State of Vermont's historic interest in protecting consumers and regulating use of sensitive data. As set forth in more detail below, certain types of legislation in this area would not conflict with federal law.

C. Areas Subject to Both State and Federal Regulation

Unfair and Deceptive Acts and Practices

The general prohibitions against Unfair and Deceptive Acts and Practices (UDAP) in commerce found in the Federal Trade Commission Act, 15 U.S.C. § 45, and Vermont's Consumer Protection Act, 9 VSA § 2435, have been applied to businesses for numerous violations of consumer privacy, including failure to provide reasonable data security to protect consumers' sensitive data[47] and failure to properly credential customers resulting in the sale of sensitive consumer data to identity thieves.[48]

An act is considered "unfair" if it causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves, and not outweighed by countervailing benefits to consumers or to competition. 15 U.S.C. § 45(n).

A "deceptive" act involves a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances.

Fair Credit Reporting Act

The federal Fair Credit Reporting Act of 1970 (FCRA)[49] and Vermont's "mini-FCRA"[50] generally track each other, though Vermont's law varies in some ways that are expressly noted in the federal law. FCRA serves two main purposes: ensuring the accuracy of consumer-report information, and ensuring that only those with a legitimate business need for the information can access it.

FCRA applies to "consumer reporting agencies" (CRAs) that provide "consumer reports" for specific purposes.[51] A Data Broker might be a CRA for some lines of its business and not for

[45] This authority was created in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, enacted in 42 U.S. Code § 1320d–5(d).
[46] 15 U.S.C. § 6807.
[47] *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).
[48] *U.S. v. ChoicePoint, Inc.*, N. D. Ga. Docket No. 06-cv-0198 (2006).
[49] 15 USC § 1681 *et seq.* In 2003, FCRA was amended by the Fair and Accurate Credit Transactions Act (FACTA) (117 Stat. 1952, codified to 15 U.S.C. §§ 1681-1681x). This description of FCRA incorporates the FACTA amendments.
[50] 9 V.S.A. § 2480a-n.
[51] A consumer report is any written or oral communication that bears on a consumer's credit standing, credit-worthiness, credit capacity, character, general reputation, personal characteristics, or mode of living, if it used for

others. Similarly, a Data Broker might trade in data that qualifies as a "consumer report" as well as data that does not.

For example, the FTC has stated that data sold for marketing purposes, to detect fraud, or to locate people, does not fall within FCRA.[52] The three major credit bureaus, in issuing traditional credit reports, are covered by FCRA. However, the bureaus provide other services not covered by FCRA. The Working Group is not aware of any business whose entire slate of business services is regulated by FCRA.

FCRA imposes separate obligations on the "issuer" of a report (the CRA), the "user" of a report (the prospective creditor, insurer, landlord, or the like), and the "furnisher" of the information (the business that reports its experience with the consumer to the CRA for subsequent use in reports).

Under FCRA, issuers of reports must: (1) make their consumers reports available to consumers free once a year, (2) disclose on the report the identity of all parties receiving the information, (3) investigate any disputes a consumer raises, (4) correct or delete inaccurate information, and (5) have protections in place to ensure that the consumer has approved the dissemination of a report to a user.[53]

If a user of a credit report denies credit, insurance, or employment to a consumer based on information in the report, it must: (1) inform the consumer that the denial was due to information in the report; (2) provide the name and address of the report's issuer; and (3) notify the consumer of his or her right to receive a copy of the report and dispute its accuracy.

The creditor or other merchant who furnishes information to a CRA: (1) is prohibited from knowingly reporting information with errors to a CRA; (2) must correct any known errors; (3) must notify the CRA of any dispute the consumer has initiated; and (4) must investigate any disputed information and report any deletions of inaccurate information to all recipients of the inaccurate information.

Vermont's mini-FCRA primarily differs from federal law in that a consumer's consent for a business to release a credit report is generally assumed to apply to all affiliates of the business under federal law.[54] In Vermont, separate consent must be obtained for each affiliate.[55]

---

one of five "permissible purposes:" for credit, for employment, for insurance, to a governmental agency (e.g., for a license or other benefit), or to a person with a legitimate business need for the information in a transaction with the consumer. *Id.* A "consumer reporting agency" is defined as "any person which...regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties." *Id.*

[52] FTC 2014 Report at i.

[53] This is a description of key elements of FCRA, not the entirety of the obligations.

[54] 15 U.S.C. § 1681t.

[55] 9 V.S.A. § 2480e.

D. State Laws Without Direct Federal Counterparts

Security Breach Notice Acts

Forty-nine states, including Vermont,[56] have Security Breach Notice Acts, which require businesses and state entities to provide notice to consumers, and in Vermont to the AGO or DFR, when the business experiences a security breach. There is no equivalent federal law.

Security Breach Notice Acts apply when certain types of data ("Personally Identifiable Information" or "PII") is believed to have been improperly acquired. In Vermont, PII means a name or first initial and last name, when combined with: (i) Social Security number; (ii) motor vehicle operator's license number or nondriver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or (iv) account passwords or personal identification numbers or other access codes for a financial account.

Vermont's Act requires businesses to notify the AGO or DFR of a breach within 14 business days of discovery of the breach, and to notify consumers in the most expedient time possible and without unreasonable delay, but no later than 45 days after the breach. The penalty for violating Vermont's Security Breach Notice is up to $10,000 per consumer.

Other states protect additional information such as a consumer's username and password, or biometric information. The applicability of such laws to security breaches in the Data Broker arena is more fully discussed in Section III.F.

Social Security Number Protection Act[57]

Vermont's Social Security Number Protection Act limits how businesses can use a consumer's Social Security Number (SSN). For example, they cannot: intentionally communicate someone's SSN to the public; require someone to transmit his or her SSN over the internet except via a secure or encrypted connection; print someone's SSN on a card used to access products or services; print someone's SSN on materials that are mailed to him or her (with some exceptions); or sell or disclose someone's SSN without written consent.

Document Safe Destruction Act[58]

Vermont's Document Safe Destruction Act requires businesses to take all reasonable steps to destroy consumers' records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable.

[56] 9 V.S.A. §§ 2430-35.
[57] 9 V.S.A. § 2440.
[58] 9 V.S.A. § 2445.

This law exempts businesses subject to HIPAA, GLBA, and FCRA, described below.

California's Protections for Domestic Violence, Assault, and Stalking Victims

California, by statute, has created a program similar to Vermont's Safe at Home Program.[59] What is unique about California's statute is that it permits program participants to opt out of Data Broker databases. It also creates a private right of action for program participants against third parties who post or sell certain information about the participant online with the intent to cause harm to the participant,[60] with criminal penalties for persons who post information about program participants with intent to cause *imminent* harm.[61]

E. Federal Laws Without Direct State Counterparts:

The FTC's Telemarketing Sales Rule (TSR)[62] which implements the Do Not Call Registry[63]

The FTC's Do Not Call Registry is a list to which consumers may submit their telephone numbers. Telemarketers are generally prohibited from calling numbers on the Do Not Call Registry, with some exceptions. Telemarketers must check the registry every 31 days to confirm that no numbers on their call lists are in the registry. Political organizations, charities, surveyors, and businesses that have established a relationship with the consumer in the previous 18 months are excluded from this requirement.

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

Under the statutory authority of HIPAA, the U.S. Department of Health & Human Services ("HHS") promulgated a Privacy Rule which controls how health care providers can share medical information. It limits with whom health care providers and other medical entities (called "covered entities") can share patients' medical information, and gives rights to patients to examine and copy their health records and to request corrections.[64]

Importantly, HIPAA puts controls on the covered entities, not on the data itself. In other words, it is legal for non-covered entities to trade in sensitive medical data, which can be acquired or extrapolated from sources other than covered entities.[65]

---

[59] Cal. Gov. Code § 6205 – 6210.
[60] *Id*. § 6208.1.
[61] *Id*. § 6208.2.
[62] 16 CFR 310; a thorough explanation of the TSR can be found at https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule; a guide for consumers can be found at https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule.
[63] https://www.donotcall.gov/.
[64] 45 CFR Part 160; Part 164 Subparts A and E.
[65] FTC 2014 Report, fn 41; Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Scientific American, Feb. 1, 2016, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

Children's Online Privacy Protection Act of 1998 (COPPA)[66]

COPPA required that the FTC create a Rule (the COPPA Rule)[67] which gives parents control over what information is collected from young children online. The COPPA Rule applies to operators of websites and mobile apps that are directed to children under 13 that collect personal information from children, or general websites that have actual knowledge that they are collecting information from children under 13. These operators must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
- Provide parents access to their child's personal information to review and/or have the information deleted;
- Give parents the opportunity to prevent further use or online collection of a child's personal information
- Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security;
- Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.[68]

Federal Education Rights and Privacy Act (FERPA)

FERPA provides rights to parents to inspect and request corrections to students' education records. FERPA is administered by the U.S. Department of Education**.** The rights transfer to a student when he or she turns 18. FERPA also requires schools to obtain written permission from the parent or 18-year-old student before releasing information from the student's record.[69]

Schools may disclose "directory" information without consent, but must tell the parent/student first and give them the opportunity to opt out of the disclosure. Directory information includes name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.[70]

---

[66] 15 U.S.C. § 6501–6505.
[67] 16 CFR Part 312.
[68] *See also* F.T.C., Complying with COPPA: Frequently Asked Questions, www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[69] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.33.
[70] *Id*.

Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA)

GLBA applies to financial institutions and requires disclosure of privacy policies, the right of consumers to opt out of sharing their data with nonaffiliated third parties, and prohibits the sharing of customer account numbers with nonaffiliated third parties for marketing purposes.

In addition, the Electronic Fund Transfer Act requires disclosures about data sharing when a consumer makes a fund transfer.[71] The Right to Financial Privacy Act prohibits some disclosures of financial records to the federal government.[72]

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003[73]

The CAN-SPAM statute, enforced by the FTC, is often listed as a privacy law but primarily gives businesses clear guidelines on what they can, cannot, and must do in email. Penalties for violation are up to $40,654 for each separate email. CAN-SPAM requires that for all commercial messages: header information cannot be false or misleading; subject lines cannot be deceptive; if the message is an ad it must be identified as such; the message must include the sender's physical postal address; the message must include instructions on how to opt out of future email; and opt-out mechanisms must continue work for at least 30 days after the messages is sent and opt-out requests must be honored within 10 days; and if another company is handling a business's email, the business must monitor what the other company is doing on its behalf.[74]

F. The European Regulatory Regime:

In May 2018, a significant privacy regulatory regime called the General Data Protection Regulation (GDPR) will begin to be enforced in the European Union (EU). Any Data Broker, wherever headquartered, if it has a European presence and collects or processes personal data from EU residents, or processes personal data on behalf of a business that holds EU residents' data, will be subject to the GDPR. The GDPR also applies to certain Data Brokers with no EU presence who target EU residents. This is noteworthy because Data Brokers who would be impacted by new Vermont regulations may soon be required to comply with EU regulations as far as EU Residents are concerned. The Working Group also believes it is useful to consider how a large, modernized, non-US jurisdiction is confronting these issues.

[71] 15 U.S.C. § 1693 *et seq.*
[72] 12 U.S.C. §§ 3401 – 3422.
[73] FTC Rule: 16 C.F.R. § 316.
[74] *See also* F.T.C., CAN-SPAM Act: A Compliance Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

While the GDPR is too extensive to fully summarize here, its most notable features include:

- Citizens have a right to access any Personal Data[75] about them that is held by Data Controllers (an entity holding Personal Data), and to receive a free copy.
- Under certain circumstances, citizens may require Data Controllers to erase all data about the citizen; this is called "the right to be forgotten" or "data erasure."
- Before using a subject's personal data, the Data Controller must either obtain the subject's consent, and consent must be "freely given, specific, informed and unambiguous" or there must be a balancing of the individual's rights against the business interests of the Data Broker. The GDPR clarifies that "Silence, pre-ticked boxes or inactivity," is presumed inadequate to confer consent. The consent must also be specific to each data processing operation. In other words, if a business obtains a subject's consent to use data for one purpose, and then it or any downstream business wants to use it for a different purpose, it must obtain a separate consent from the subject. The use of Sensitive Personal Data requires "explicit consent," which is a higher requirement than standard consent.
- Parental consent is required before using data about children ages 16 and under, or a lower age (which can be determined by a member state).
- If a business uses scoring, it cannot solely rely on a computerized algorithm for decision-making if the decision can have a legal impact on individuals (such as a discriminatory impact)
- The GDPR includes standards of appropriate data protection of personal data, with higher standards for sensitive personal data.
- The GDPR requires notice of security breaches to the entity's country's "Supervisory Authority" within 72 hours of the breach involving any personal data.
- There are two levels of penalty under GDPR – violation of certain technical provisions, including breach notifications, permits fines up to the greater of 10 million euro (roughly $11.7M) or 2% of the company's prior year's global annual revenue. Other violations, including those relating to consent, permit fines of up to 20 million euro (roughly $23.3M) or 4% of the company's prior year's global annual revenue.

[75] "Personal Data," which is the key definition, is very broad, and means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, IP address, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

"Sensitive Personal Data," for which additional protections and restrictions apply, means "personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data."

G. Proposed legislation at the federal level or in other states

In response to heightened public concern regarding data security and privacy – prompted in part by the 2017 Equifax breach and other recent high-profile data-security incidents – legislatures and regulators across the country in recent years have considered, or are currently considering a variety of measures to protect consumers.

For example:

A number of states have enacted or are proposing legislation this year eliminating credit-freeze fees.[76]

In California, a bill relating to Data Brokers, SB-1348,[77] was introduced in 2014. This bill would have permitted consumers to review the information a Data Broker collected about the individual and to opt out of having that information shared. It required Data Brokers to clearly and conspicuously post their opt-out procedures. This bill did not pass.

Bill S.1815 was introduced in the U.S. Senate on September 14, 2017. This bill would give consumers the right to review and correct information collected by Data Brokers and to opt-out of sharing certain information for marketing purposes. The bill requires Data Brokers to establish procedures to ensure the accuracy of the information they collect and to implement comprehensive consumer privacy and data security programs. It also prohibits Data Brokers from obtaining personal information by false pretenses.

Previously, elements of this bill were introduced as S.668 in 2015 and S. 2025/H.R. 4516 in 2014. S.1995, introduced in 2014, addressed data breaches and also had data security standards language for Data Brokers. None of the bills have passed to date.

[76] The Working Group is aware of proposed legislation in at least three other states. There will likely be others. A complete list of current credit freeze laws can be found at http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx.

[77] Cal. Leg. SB-1348, Data brokers: sale of personal information (Feb. 21, 2014), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1348.

V. Recommendations

A. Definition of "Data Broker"

Act 66 requires the Working Group to propose "an appropriate definition of the term 'data broker.'"

The Working Group received a great deal of comment on the potential definition of the term. Many commenters suggested a narrow approach, to ensure that entities that hold data only incidentally — i.e. not as their primary business — would not be swept up.

The Working Group believes that any definition of data broker should encompass the following concepts:

1. A Data Broker is an entity that collects data about consumers, primarily for the purpose of selling that data or analytic scores based on that data.

   A Data Broker might take an interim step of analyzing, repackaging, cleaning, or otherwise manipulating the data, but the key element is that a data broker both collects and sells the data, and this is the primary purpose of the data collection.

2. A Data Broker does not have a direct relationship with the customer, user, or employee whose data is being collected.

   Some of the most prevalent consumer concerns about Data Brokers derive from the fact that consumers generally do not know who is handling their data, and cannot contact the data broker to have their information removed or corrected.

   Accordingly, the following businesses fall outside of the scope of the proposed definition of data broker, as the data they are collecting is from their own customers, and the customers therefore have some level of knowledge and control over the fact that their data is being collected, and the ability to opt out:[78]

   - Banks and other financial institutions
   - Utilities
   - Insurers
   - Retailers and Grocers
   - Restaurants and Hospitality Businesses
   - Social Media Websites and Mobile Apps

[78] In reality, often consumers may be unaware that the businesses with whom they directly do business are collecting and reselling their data, or to whom they are reselling it, or what the full implications of that resale are. Furthermore, many companies do not offer an "opt out," and given the widespread information sharing, any consumer attempting to avoid any business that resells his or her data would essentially have to opt out of e-commerce and use of the internet, which is not reasonable in the modern economy. However, for the purposes of focusing this legislation, the Working Group believes this distinction is important.

- Search Websites
- Businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as website, app, and e-commerce platforms

Working Group's Recommended Definition of "Data Broker"

A commercial entity that (1) assembles, collects, stores, or maintains personal information concerning individuals who are not customers, users, or employees of that entity, and (2) sells the information to third parties.

B. Regulation of Data Brokers

The Working Group recommends that the General Assembly consider adopting several measures that will provide consumers with significant protections, but will not place an undue burden on the Data Broker industry. The suggested legislation also addresses some of the current regulatory weaknesses that have been exposed by the Equifax breach. The Working Group also received additional recommendations for regulation through public comment, which are included in Exhibit A.

The Working Group recommends for the Legislature's consideration the following legislative potential actions:

1. Amend Vermont's credit-freeze law (9 V.S.A. § 2480h) to prohibit credit reporting agencies from charging a fee to freeze or unfreeze consumers' credit reports;
2. Provide consumers with more information about opt-out rights and how to exercise them, by requiring Data Brokers to provide the State of Vermont with certain information;
3. Create new causes of action, enforceable by a consumer or the Attorney General, against those who acquire data with the intent of committing certain wrongful acts;
4. Require Data Brokers to employ reasonable security methods to protect data;
5. Require Data Brokers that suffer certain data breaches to quickly provide notice of the breach;
6. Protect children by prohibiting the sale of data about certain minors without parental consent.

The first recommendation amends existing law. The latter parts should be added to Title 9 in Chapter 62: Protection of Personal Information.

While further legal analysis and discussion is required, the Working Group's preliminary research and legal analysis indicates that the litigation risk involved in the first three considerations is relatively low. The latter three may involve more substantial risks that the Assembly will want to carefully consider, in consultation with legislative counsel, DFR, and the

AGO, in determining whether the potential benefits to the public outweigh the risks to the State.

1. Credit Freeze Fee

Under current law, any Vermont consumer may place a security freeze on his or her credit report.[79] A credit reporting agency may not charge a fee to victims of identity theft, and for others may charge a fee of no more than $10.00 to freeze a report, and no more than $5.00 to remove the freeze. Requests to freeze credit reports must be made by certified mail. Victims of identity fraud must accompany the request with a copy of a police report, investigative report, or complaint that the consumer has filed with a law enforcement agency regarding the unlawful use of personal information.

The Working Group recommends that the General Assembly prohibit credit reporting agencies from charging a fee to any consumer who wishes to freeze or unfreeze his or her credit report. A victim of identity theft should not have to provide additional documentation of a theft to avoid paying a fee, as is required under current law. Such documentation is typically only available after a theft has occurred, and the real value of a credit freeze is to prevent identity theft, not to respond to it. Given that consumers rarely have a meaningful choice as to whether their data is collected, and it is largely the agencies who benefit from having the data, consumers should not have to pay the agencies for freezing and unfreezing their own data.

Three states already prohibit such fees: Indiana, Maine, and South Carolina.[80] Some states prohibit freeze fees for senior citizens. The Working Group understands that other states are currently considering legislation that would prohibit such fees. Federal legislation was proposed shortly after the 2017 Equifax breach, but it has not been enacted.

2. Increase Consumer Awareness of Data Broker Opt-Out Rights

One way to address consumer's privacy concerns is to better inform consumers of their opt-out rights. Several commenters recommended that the State provide an easier means for consumers to both learn about and exercise their opt-out rights.

Some Data Brokers already allow consumers to opt out of having their data shared. For example, the Data & Marketing Association (the "DMA"), a leading industry trade-group for data brokers, sets and maintains ethical guidelines for its members. *DMA Guidelines for Ethical Business Practice* ("DMA Guidelines").[81] The DMA Guidelines expressly state that: "A DMA Member: Honors requests not to have personally identifiable information transferred for marketing purposes."[82] Article 31 of the DMA Guidelines is to the same effect. Id. at 20. The

[79] 9 V.S.A. § 2480h.
[80] See Ind. Code § 24-5-24-14; Me. Rev. Stat. Tit. 10 § 1310(1)(A)(2); S. Carolina Code § 37-20-160(J).
[81] DMA, *Direct Marketing Association Guidelines for Ethical Business Practice*, https://thedma.org/wp-content/uploads/DMA-Guidelines-2016.pdf.
[82] *Id.* at 3.

Working Group heard testimony from both consumer advocacy groups and Data Brokers that requests for opt-out are generally honored.

However, most consumers do not know how to make such a request to the brokers that hold their data. Consumers, in fact, likely do not know who the brokers are, or how to go about contacting them and opting out of their lists. When the DMA testified before the House Commerce and Economic Development Committee, it was directly asked for a list of its membership and declined to provide one. Even when a consumer is aware of who holds their data, and how to contact them, it is difficult for a consumer to verify that their opt-out request has been honored.

To simplify this process and provide greater transparency for consumers, the Working Group recommends that Data Brokers be required annually to provide the following limited information to the State:[83]

1. The Data Broker's corporate name and primary physical, email, and web addresses.
2. If the Data Broker permits consumers to opt out of its databases or to opt out of certain sales of data:
    a. The method(s) for requesting the opt-out;
    b. If only certain sales are covered, which ones;
    c. Whether the Data Broker permits consumers to authorize a third-party to perform the opt-out in their stead.
3. If the Data Broker does not permit consumers to opt out, a statement that it does not permit opt-outs.

3. <u>Prohibit Acquisition of Data for Illegal Purposes</u>

One of the significant dangers of the broad availability of personal data is that it can be used with malicious intent to facilitate wrongful acts such as discrimination, stalking, harassment, fraud, or identity theft. While various criminal and civil statutes bar these practices, there is currently no prohibition on *acquiring* data for the purpose of committing these wrongful acts. The Working Group recommends that the General Assembly adopt legislation that would make it illegal to acquire personal data for the purpose of:

1. Stalking or harassing;
2. Identity theft;
3. Financial fraud;
4. Email fraud;
5. Employment discrimination; or
6. Housing discrimination.

[83] The Working Group has identified the Secretary of State as an official who currently performs a similar function in other areas (e.g. the Corporations Database) and may have an infrastructure to build on. The Working Group recommends that the Legislature consult with the Secretary of State regarding the resources required to securely and effectively implement this recommendation.

Creating a cause of action — enforceable by State's Attorneys, the Attorney General or consumers — will set a clear standard that bad actors should not use information garnered from data brokers to facilitate other wrongs. It will also provide an additional, earlier authority for the Attorney General or a consumer to take legal action to prevent the wrong before it happens.

4. Minimum Data Security

Even large and sophisticated Data Brokers can have deficient data security, as evidenced by the 2017 Equifax breach and other breaches described above. The Legislature should consider requiring expressly that data brokers must adequately secure sensitive data. To date, states[84] and the FTC have prosecuted unreasonable data security as an unfair or deceptive act under the FTC Act or state Consumer Protection Acts. One criticism of this approach is that it does not provide pre-violation guidance as to what "reasonable" data security is.

The Commonwealth of Massachusetts has addressed this issue by setting minimum data security standards, which apply to all businesses that handle certain highly sensitive personal information.[85] While Massachusetts has the most detailed standards, which are set forth in a regulation, fourteen other states have laws that generally require that businesses who handle personal information "implement and maintain reasonable security procedures" or similar requirements.[86] The Working Group proposes that Vermont consider adopting a standard similar to Massachusetts, either with regard to all businesses handling PII, or only with regard to Data Brokers.

In Massachusetts, any entity that owns or licenses personal information about any Massachusetts resident must "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards" that are appropriate based on a variety of factors (size and type of business, nature and amount of data, available resources). The regulation requires compliance with any data security requirements applicable to the data or the entity holding it. The regulation also imposes more specific requirements concerning risk assessment, oversight of employees and contractors, employee

[84] Multistate enforcement actions regarding failure to adequately secure sensitive data have recently resulted in Assurances of Discontinuance with Target (48 States, available at https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over), Adobe Systems Inc. (15 states, available at http://www.illinoisattorneygeneral.gov/pressroom/2016_11/20161110.html), and Nationwide Mutual Insurance Company (34 states, available at http://ago.vermont.gov/focus/news/attorney-general-announces-nationwide-data-breach-settlement.php).

The State of Vermont has also entered into several non-Multistate settlements with businesses that failed to provide adequate security, including SAManage Inc. (available at http://ago.vermont.gov/focus/news/attorney-general-settles-data-breach-case-for-$264000-issues-$400-per-social-security-number-penalty.php) and Hilton Domestic Operating Company Inc.(available at http://ago.vermont.gov/focus/news/vermont-attorney-general-resolves-security-breach-with-hilton-company-to-pay-$300000-penalty.php)

[85] 201 Code of Mass. Regs. 17.01 – 17.05; *see* Mass. Gen. L. Ch. 93H, § 2(a) (authority for regulations).

[86] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

training, and the like. Finally, the regulation imposes even-more specific requirements on regulated entities' computer systems and access thereto. The Massachusetts standards have been in effect since 2010 and are reproduced in Exhibit B.

5. Swift Notice of Security Breaches

The Working Group recommends that the Legislature consider requiring Data Brokers to provide prompt notice when certain sensitive information is compromised by a security breach. Prompt notice of a breach is important so that consumers can take steps to protect themselves. Depending on the information that a Data Broker has, a Data Broker breach may be particularly sensitive because it will likely to lead to identity theft and fraud. Moreover, because Data Brokers' primary business is, by definition, the acquisition, storage, and sale of data, they may reasonably be held to a higher standard than other businesses that hold data only incidentally to their primary business.

Vermont's Security Breach Notice Act, 9 V.S.A. § 2435, is insufficient to address Data Broker breaches because it is only triggered when a data collector that owns or licenses computerized Personally Identifiable Information (PII)[87] is breached. For example, an entity that had the following types of data breached would not be required to report a breach under current Vermont law because the data is not PII:

- Name plus health care information, list of treatments (this information can be derived from purchase history and searches, and is also not covered by HIPAA);
- Name, address, phone, family history and names of relatives, income, assets, and liabilities; or
- Social security number, driver's license number, passport number, age, or address, without a name (however, such "deidentified" data can easily be re-connected with a name).

In addition, the Security Breach Notice Act requires notice "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery."[88] Equifax provoked widespread outrage because many felt that the notice was given too late. The Working Group believes that it would be appropriate to strengthen the notice requirement for Data Brokers, given that their primary business is the acquisition, storage, and sale of data, and because of the potential harm to consumers associated with delay.

The Working Group does not recommend expanding the existing Vermont Notice Act, as that Act covers all businesses that collect data, not just Data Brokers. Data Brokers are differently situated from other businesses that hold sensitive data, and accordingly it is appropriate to regulate them differently. However, the proposed Data Broker Security Breach Notice Act should closely track the language of the Vermont Notice Act, for simplicity in implementation.

[87] Personally Identifiable Information is defined in fn 25.
[88] 9 V.S.A. § 2435(b)(1).

The Working Group recommends that the Legislature consider a Data Broker Security Breach Notice Act consistent with the existing Notice Act, except:

- Applies only to Data Brokers;
- Applies to breaches involving "Data Broker Personal Information" ("DBPI"), a definition which would draw from the broader PII definition found in FERPA;
- Requires notice to the Attorney General's Office;
- Requires that notice include a description of all categories of data acquired;
- Currently, under subpart (d)(1) of the Vermont Notice Act, a business that believes that "misuse of personal information is not reasonably possible" can notify the AGO or DFR and if the agency agrees with the determination, no notice will be necessary. The Data Broker version would also have the words "or the likelihood of identity theft is extremely low" or words to that effect.

6. Protecting Children

The Working Group heard testimony that protections for data about children are quite limited under current law. The Working Group's research confirms this to be the case.

Federal law covers some sharing of information about children, but the laws are limited in scope. As discussed above, FERPA addresses certain information about students collected by schools receiving federal funds, and requires parental consent for release of any such information for commercial purposes.[89] COPPA addresses information supplied to websites for children under 13.[90] However, there is no federal protection for non-school data about children between 13 and 18 years old, and no protections for data about children obtained through surveys, purchase history, write-in contests, or the like. Furthermore, if an unscrupulous website does collect a child's data in violation of the law, once the data is in the hands of data brokers its source or origin may be lost and there is nothing stopping the subsequent resale of that data.

The working group recommends that the Legislature consider prohibiting the sale of any sensitive data collected outside of school about children between the ages of 13 and 18 without the written permission of the child's parent or guardian, except for limited purposes. Because there are several potential areas of litigation risk, the Working Group recommends that the Legislature work closely with Legislative Council and the Attorney General's Office in drafting such legislation.

[89] See 20 U.S.C. § 1232g(b) (FERPA prohibition on certain releases of student data); 34 C.F.R. § 99.33 (regulatory description of FERPA limitation on disclosure of student information).

[90] See 15 U.S.C. § 6501(1) (COPPA definition of "child" as anyone under age 13); *id*. § 6502(d) (COPPA preempts state law only to the extent that it is inconsistent with the treatment of activities governed by COPPA). Because COPPA governs only activities involving children under 13 it does not preempt state laws concerning teenagers.

Bibliography

All documents have been archived at http://www.ago.vermont.gov/news-and-updates/data-broker-working-group1/data-broker-working-group-documents-referenced.php.

1. 2017 Vt. Acts & Resolves No. 66.

2. Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Scientific American, Feb. 1, 2016, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

3. Andriotis, AnnaMaria et al., *Senators Rip Credit-Reporting Model in Wake of Equifax Breach*, Wall St. J., Oct. 4, 2017, https://www.wsj.com/articles/senators-rip-credit-reporting-model-in-wake-of-equifax-breach-1507136171.

4. Angela Moscaritolo, *LexisNexis admits to another major data breach*, SC Magazine, May 4, 2009, https://www.scmagazine.com/lexisnexis-admits-to-another-major-data-breach/article/555843/.

5. Anna North, *When a SWAT Team Comes to Your House*, N.Y. Times, Jul. 6, 2017, https://www.nytimes.com/2017/07/06/opinion/swatting-fbi.html.

6. Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KrebsOnSecurity, Sep. 25, 2013, https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

7. Brian Krebs, *Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records*, KrebsOnSecurity, Mar. 10, 2014, https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/

8. Brian Krebs, *Feds Indict Three in 2011 Epsilon Hack*, KrebsOnSecurity, Mar. 15, 2006, https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/.

9. Cal. Leg. SB-1348, Data brokers: sale of personal information (Feb. 21, 2014), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1348

10. Complaint, *Massachusetts v. Equifax* (Sept. 19, 2017), http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf.

11. DMA, *Direct Marketing Association Guidelines for Ethical Business Practice*, https://thedma.org/wp-content/uploads/DMA-Guidelines-2016.pdf.

12. Exec. Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016.

13. Exec. Office of the President, President's Council of Advisors on Sci. and Tech., *Big Data and Privacy: A Technological Perspective*, May 2014.

14. F.T.C., CAN-SPAM Act: A Compliance Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

15. F.T.C., Complying with COPPA: Frequently Asked Questions, www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

16. F.T.C., Complying with the Telemarketing Sales Rule, https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule

17. F.T.C., *Data Brokers, A Call for Transparency and Accountability*, May 2014.

18. F.T.C., *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003*, Dec. 2012.

19. F.T.C., The Telemarketing Sales Rule, https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule.

20. Farhad Manjoo, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. Times, Sept. 8, 2017, https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html.

21. Geoffrey A. Fowler, *Your Data is Way More Exposed than You Realize*, Wall St. J., May 24, 2017, https://www.wsj.com/articles/your-data-is-way-more-exposed-than-you-realize-1495657390.

22. Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. Times., Apr. 13, 2005, https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html.

23. John Leyden, *Acxiom database hacker jailed for 8 years,* The Register, Feb. 23, 2006, https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/

24. Juan Carlos Rodriguez, *LexisNexis Could Have Suffered Data Breach, FBI Says*, Law360, Sept. 26, 2013, https://www.law360.com/articles/475918/lexisnexis-could-have-suffered-data-breach-fbi-says.

25. L. Sweeney, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon Univ., Data Privacy Working Paper 3. Pittsburgh 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf.

26. Miguel Helft, *After Breach, Companies Warn of E-Mail Fraud*, N.Y. Times, Apr. 4, 2011, Retrieved from https://www.nytimes.com/2011/04/05/business/05hack.html.

27. Nat'l Network to End Domestic Violence, *People Searches and Data Brokers,* 2013, https://nnedv.org/mdocs-posts/people-searches-data-brokers/.

28. Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous'* People, N.Y. Times, Jan. 29, 2015, https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.

29. Press Release, F.T.C., *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers,* Feb. 18, 2016, www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

30. Press Release, F.T.C., *FTC Puts An End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts*, Nov. 30, 2016, www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

31. Press Release, Ill. Att'y Gen., *Attorney General Madigan Announces $1 Million Settlement with Adobe*, Nov. 10, 2016, http://www.illinoisattorneygeneral.gov/pressroom/2016_11/20161110.html.

32. Press Release, N.Y. Att'y Gen., *A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach*, May 23, 2017, https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

33. Press Release, Vt. Att'y Gen., *Attorney General Announces Nationwide Data Breach Settlement*, Aug 9, 2017, http://ago.vermont.gov/focus/news/attorney-general-announces-nationwide-data-breach-settlement.php.

34. Press Release, Vt. Att'y Gen., *Attorney General Settles Data Breach Case for $264,000; Issues $400 Per Social Security Number Penalty*, Sep. 29, 2017, http://ago.vermont.gov/focus/news/attorney-general-settles-data-breach-case-for-$264000-issues-$400-per-social-security-number-penalty.php.

35. Press Release, Vt. Att'y Gen., *Vermont Attorney General Resolves Security Breach with Hilton Company to Pay $300,000 Penalty*, Oct. 31, 2017, http://ago.vermont.gov/focus/news/vermont-attorney-general-resolves-security-breach-with-hilton-company-to-pay-$300000-penalty.php.

36. Senate Comm. On Commerce, Science & Transp., Staff Rep. for Chairman Rockefeller, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Dec. 18, 2013.

37. Stacy Cowley and Tara Bernard, *As Equifax Amassed Ever More Data, Safety was a Sales Pitch*, N.Y. Times, Sept. 23, 2017, https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html.

38. Transcript of Waiver of Indictment and Plea to Information Hearing, *U.S. v. Hieu Minh Ngo*, Docket No. 1:12-cr-00144 Doc. 27, Mar. 7, 2014.

39. United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, June 30, 2014.

40. World Privacy Forum, *Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?*, Dec. 18, 2013.

41. World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future,* April 2, 2014.

Exhibit A: Stakeholder Recommendations

This exhibit summarizes the recommendations made by stakeholders and interested parties through testimony and comments submitted to the Working Group.[91]

Some parties made recommendations that the Working Group have included in part or whole in its proposal to the General Assembly. A number supported the idea of a Data Broker Clearinghouse or registration with the state.[92] Some recommended that the state require Data Brokers to adhere to minimum security standards.[93] Two recommended a prohibition on the use of data to discriminate or otherwise break the law.[94]

Stakeholders also made the following recommendations that were not included in the Working Group's proposal.

1. No Legislative Change

Some stakeholders opined that no legislative change is necessary because the industry currently has sufficient self-regulation, industry members are aware of potential harms and have taken steps to mitigate those harms, and regulation could have harmful unintended consequences. These stakeholders did not propose any alternatives for legislators to consider.

This recommendation was made by Acxiom, the Coalition for Sensible Public Record Access (CSPRA); the Consumer Data Industry Association (CDIA); Computing Technology Industry Association (CompTIA); RELX Group (owner of LexisNexis); and TechNet.

2. Consumer Right to Know and Disclosures

The most common recommendations involved information that consumers should be allowed to discover about the Data Brokers that collect their data. Proposals suggested that Data Brokers should be required to either affirmatively disclose this information or make it available on request. Some recommendations related to general information about Data Brokers' practices, others to individual consumer rights regarding to their own specific data.

These commenters suggested that a Broker should be required to clearly and conspicuously disclose:

---

[91] All submitted comments can be found at http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-broker-working-group.php.

[92] This recommendation was made by Consumer Action, Consumer Federation of America (CFA), Consumer Watchdog, the National Consumers League (NCA), PrivacyMate, Privacy Rights Clearinghouse, Prof. N. Cameron Russell of Fordham University School of Law, and the Vermont Public Interest Research Group (VPIRG).

[93] This recommendation was made by Consumer Action, CFA, Consumer Watchdog, NCA, PrivacyMate, and Privacy Rights Clearinghouse.

[94] This recommendation was made by Amnesty International and Prof. Chris Jay Hoofnagle of the University of California Schools of Information and School of Law.

- The names and contact information of third-parties with whom the Data Broker shares information;
- the purposes for which the information is sought and sold;
- the types of lists and "categories" of consumers that the Data Broker sells; and
- the sources of the information that the Data Broker collects.

These commenters also suggest that Data Brokers should be required to provide to any Consumer who requests it:

- a complete copy of all the information collected about the consumer;
- an audit or disclosure log to determine how data about the consumer has been sold and to whom;
- the various "categories" that the consumer has been assigned into and why.

These recommendations were made by the American Civil Liberties Union (ACLU), Amnesty International, Consumer Action, Consumer Federation of America (CFA), Consumer Watchdog, Prof. Chris Jay Hoofnagle of the University of California Schools of Information and School of Law, the National Consumers League (NCA), PrivacyMate, Privacy Rights Clearinghouse, Prof. N. Cameron Russell of Fordham University School of Law, and the Vermont Public Interest Research Group (VPIRG). This is a summary of the recommendations. Some of these stakeholders proposed a subset of the recommendations above.

3. Opt-Out

Several stakeholders recommended that Data Brokers be required to establish an opt-out procedure for sharing information with third-parties. Some advocated further that any such opt-out procedure be free-of-charge. Some stakeholders recommended this option be limited to data used for marketing purposes or people search products. One stakeholder recommended the opt-out be the default, and consumers have the option to opt in to allow Data Brokers to collect, store, and share their data.

The following recommendations would apply to either a newly created opt-out requirement, or to the existing opt-out procedures that some Data Brokers already have:

- Opting out be available to individuals in a one-step process encompassing all Data Brokers listed in the clearinghouse;
- No personal information provided to a Data Broker for the purpose of opting out may be used by the Data Broker to add to its profile on that individual; and
- Fees to opt out be prohibited.

These recommendations were made by the ACLU, CFA, NCA, Consumer Watchdog, Consumer Action, Vermont Consumer Assistance Program (a division of the Attorney General's Office that did not participate in the Working Group), the Vermont Network Against Domestic & Sexual Violence, PrivacyMate, and Privacy Rights Clearinghouse.

Privacy Rights Clearinghouse also recommended adoption of a law like one existing in California which provides participants in the Secretary of State's confidential address program, Safe at Home (for victims of domestic violence or stalking and reproductive health care providers, employees, and volunteers) with the right to demand the removal of their personal information, including home address and phone number, from online search engines or databases, and imposes related obligations on the operators of such search engines and databases. Cal. Gov. Code § 6208.1.

4. FCRA rights: Right to Review and Correct, and Adverse Action Reporting

Several stakeholders recommended that Data Brokers provide a method for consumers to review and correct information that the Data Brokers maintain about the consumers, similar to requirements under FCRA regarding credit reports. The comments recommend that instructions on how to exercise these rights should be clearly and conspicuously posted on each Data Broker's website.

Comments concerning this recommendation suggested that entities that decline to transact with a consumer based on information provided by a Data Broker for fraud mitigation purposes should be required to provide the consumer with a basic explanation of the nature of that data and how to reach the Data Broker that supplied it, similar to requirements under FCRA regarding adverse actions.

These recommendations were made by the ACLU, Amnesty International, CFA, NCA, Consumer Watchdog, Consumer Action, PrivacyMate, Privacy Rights Clearinghouse, and VPIRG.

5. Deidentification and Anonymization

Two stakeholders recommended that Data Brokers that de-identify data should be required to disclose their de-identification technique so that it is understandable, and further that there be a clear link established as to how this degree of de-identification protects privacy, and a disclosure of the perceived risk of re-identification.

These comments also suggest that legislation:

- Prohibit as deceptive the practice of calling data "anonymous" or de-identified where data brokers and their clients can re-identify or otherwise link the data to individuals;
- Prohibit data brokers from re-identifying datasets that were collected under promises of privacy or anonymity; and
- Prohibit data brokers from coaching clients to collect data in misleading ways (for an example, look at the reverse enhancement battle in California, where data brokers coached clients to collect zip codes because consumers would not realize that zip codes were personally identifiable).

These recommendations were made by the Electronic Frontier Foundation (EFF) and Hoofnagle.

6. Regulation of Data Providers

Two stakeholders recommended that Companies that provide data to Data Brokers ("Data Providers") should be specifically required to disclose this fact to consumers. The comments further provide that Consumers should be able to opt out/opt in to transfer of data from Data Providers to Data Brokers.

These recommendations were made by Hoofnagle and VPIRG.

7. Credentialing

One comment provided that Data Brokers should be required to screen clients' use of their services and refuse to provide services where the client is engaged in deceptive marketing, stalking, or other illegal behavior.

Data Brokers could give notice of, or share liability, where a client of a Data Broker uses personal information to defraud consumers.

This recommendation was made by Hoofnagle.

8. Respect for Human Rights

One comment recommended that Vermont should make explicit that Data Brokers have a responsibility under the UN Guiding Principles on Business and Human Rights to exercise human rights due diligence to identify, prevent, mitigate and account for the potential human rights risks of their operations. Data Brokers should have systems in place to prevent the company from contributing to human rights abuses.

This recommendation was made by Amnesty International.

9. Government Transparency

One comment recommended that Vermont government agencies that purchase data from data brokers should be transparent about their use of the products, including making contracts publicly available and taking measures to ensure that the data is accurate, and that data, or inferences, about people or groups of people will not lead to discriminatory, or otherwise unlawful outcomes.

This recommendation was made by Amnesty International.

10. Disclosures by Data Broker Customers

One comment recommended that Clients of data brokers should include "how did you get my information" disclosures on direct mail and other personalized advertisements.

This recommendation was made by Hoofnagle.

11. Public Awareness and Education

Two comments recommended that the Attorney General and Department of Financial Regulation should hold a public awareness campaign regarding how consumer information is shared, how consumers can better protect their online privacy, and how 'Do Not Track' browser options work.

This recommendation was made by the ACLU and PrivacyMate.

12. Consumer Protection Act

One comment recommended that the Attorney General should use the Vermont Consumer Protection Statute to prosecute abuses by Data Brokers.

This recommendation was made by the ACLU.

Exhibit B: Massachusetts Data Security Regulation

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements
17.05: Compliance Deadline

17.01: **Purpose and Scope**

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and

information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;

2. employee compliance with policies and procedures; and

3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: **Compliance Deadline**

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY 201 CMR 17.00: M.G.L. c. 93H