VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2015 UNIVERSITY OF VIRGINIA VOL. 19, NO. 03

How Could They Know That? Behind the Data that Facilitates Scams Against Vulnerable Americans

ALEX SCHNEIDER[†]

† Juris Doctor, The George Washington University Law School, December 2015; B.A., Brandeis University, 2012.

ABSTRACT

Scammers have discovered a powerful tool for committing fraud: data broker marketing lists. Largely unregulated, the data broker industry collects, trades, and sells personal information on the majority of Americans without their knowledge or consent. The industry has a long track record of selling highly sensitive data to shady figures, including scammers that target vulnerable seniors as part of the grandparent scam. The status quo is untenable. Data brokers should be responsible for protecting consumer data by carefully vetting list buyers. Consumers, meanwhile, should be empowered to recognize the link between data disclosure and scams, and to opt-out of data sharing. This Note identifies the strong link between the data broker industry and scams like the grandparent scam, arguing ultimately that policy makers must step in to dictate acceptable industry practices that mirror rules placed on the credit reporting industry.

TABLE OF CONTENTS

I. INTRODUCTION

Pascal Goyer and his Canadian cronies' criminal operation were systematic and organized. Working off a printout of 13,000 names of American seniors aged seventy or older, they simply ran down the list, targeting their elderly victims in what authorities call a "grandparent" scam operation.[1] Posing as the grandchildren of their victims, the scammers called seniors asking them to wire money due to an emergency situation, and enough confused grandparents complied.[2] The scammers kept notes, annotating their lists with the grandchildren they impersonated and the cash amounts they were to receive in the next wire transfer.[3]

A similar scam ring based out of Toronto used lists that were "8 or 9 inches thick" to convince seniors to shell out an estimated $3 million to help their grandkids.[4] In Montreal, a police raid of a five-man operation led to the confiscation of fifteen cell phones, $11,000 in cash, a .22 caliber revolver

---

[1] Telephone Interview with Ellyn Lindsay, Assistant U.S. Attorney, U.S. Attorney's Office, Cent. Dist. of Cal. (Mar. 18, 2014); *see also* Press Release, FBI Los Angeles, Alleged Operator of 'Grandparent Scam' Indicted (Oct. 26, 2012), http://www.fbi.gov/losangeles/press-releases/2012/alleged-operator-of-grandparent-scam-indicted.

[2] *See* Press Release, FBI Los Angeles, *supra* note 1.

[3] *Id.*

[4] Sid Kirchheimer, *Grandkids Scam Ring Busted*, AARP BULL. (Feb. 24, 2011), http://www.aarp.org/money/scams-fraud/info-02-2011/grandkids_scam_ring_busted.html; *see also* David Lea, *'Emergency Scam' ring busted*, OAKVILLE BEAVER (Feb. 23, 2011), http://www.insidehalton.com/news-story/2987474--emergency-scam-ring-busted/.

and—once again—lists of American seniors by name and telephone number.[5]

Buying these lists identifying American seniors was straightforward for these foreign fraudsters. They are the same lists that companies buy to improve marketing tactics, that political campaigns use to target potential donors, and that ad networks use to track browsing history and personal interests to better deliver targeted advertising.[6] The personal information of millions of Americans—sorted by age, interests, wealth, or location—can be aggregated into a spreadsheet with a few clicks and a credit card number.

The elusive keepers of these lists are called "data brokers," collectors, traders, and peddlers of personal information. To these brokers, information is a commodity like gasoline or silver, produced cheaply and sold at a premium.[7] Once in the hands of brokers, the information is

---

[5] *See* Cheryl Cornacchia, *West Island Call Centre Busted for Grandchild Phone Scam*, MONTREAL GAZETTE (Mar. 7, 2012), http://montrealgazette.com/news/world/west-island-call-centre-busted-for-grandchild-phone-scam.

[6] *See generally* Joel Stein, *Your Data, Yourself*, TIME, Mar. 21, 2011, at 40–46, *available at* http://content.time.com/time/magazine/article/0,9171,2058205,00.html; Lois Beckett, *How Microsoft and Yahoo are Selling Politicians Access to You*, PROPUBLICA (June 11, 2012), http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you; Alexis C. Madrigal, *I'm Being Followed: How Google—and 104 Other Companies—are Tracking Me on the Web*, THE ATLANTIC (Feb. 29, 2012), http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/.

[7] *See, e.g.*, Paul Brown, *The Year of the Dividend: What's in a Name?*, N.Y. TIMES (Dec. 9, 2006), http://www.nytimes.com/2006/12/09/business/09offline.html?pagewanted=print.

aggregated into lists or sold, without the knowledge or permission of members of the public. When companies buy or sell Internet browsing histories, grocery store preferences, home value estimates, or age categories, consumers have no knowledge of the transaction or recourse when the information proves harmful to their interests. The data broker industry operates today with impunity in a largely unregulated environment.[8] But despite nearly a decade of investigations, lawmakers and regulators have not acted.[9]

Ongoing debates between privacy advocates and companies that amass data time and again return to the basic question: what is the harm?[10] After all, the data industry argues, the worst that can happen is that a consumer gets on the wrong list and is bombarded with advertisements for unwanted products.[11] The harm has been proven, in part, by scam artists who have used these easily accessible lists, called "lead lists," as tools for committing fraud.[12] In fact, Pascal Goyer

---

[8] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 7 (2013) [hereinafter *GAO Report*].

[9] *Compare GAO Report*, *id.*, *with* ANGIE WELBORN, CONG. RESEARCH SERV., RS22087, INFORMATION BROKERS: FEDERAL AND STATE LAWS (2005).

[10] *See generally* Daniel Solove, *Privacy and Data Security Violations: What's the Harm?*, LINKEDIN (June 25, 2014), https://www.linkedin.com/pulse/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm.

[11] Letter from Linda Woolley, President and CEO, Direct Mktg. Ass'n, to the Bipartisan Congressional Privacy Caucus (Aug. 13, 2012), http://the-dma.org/news/August-13-2012-DMALetter.pdf.

[12] *See* Shelby Moore and Jeanette Schaefer, *Remembering the Forgotten Ones: Protecting the Elderly from Financial Abuse*, 41 SAN DIEGO L. REV. 505, 549 (2004).

purchased his list of seniors from InfoCanada, part of the major data broker and Direct Marketing Association member InfoGroup.[13]

Fighting crimes like the grandparent scam does not have to be a perpetual game of whack-a-mole. Data brokers should be responsible for protecting consumer data by vetting list buyers. Consumers, meanwhile, should learn about how data brokers work and should have the option of easily opting-out of systems that share their data without their permission. This Note identifies the strong link between the data broker industry and lead list scams, arguing ultimately that policy makers must take action to dictate acceptable practices related to sharing marketing lists, mimicking the successes of regulation of the credit reporting industry.

In this discussion of the dangers of data collection, I first look at the grandparent scam, its causes, campaigns to educate consumers about its dangers, and laws enhancing penalties for elder fraud. Next, I review the history of data brokers, including the various types of brokers and their sources of personal information. I discuss harms, other than those to the elderly, that these brokers present. I then look at existing laws governing data accumulation and resale, especially the Fair Credit Reporting Act. I review Federal Trade Commission enforcement actions against brokers and failed voluntary guidelines and legislative initiatives, as well as education campaigns.

---

[13] Interview with Ellyn Lindsay, *supra* note 1. An official from InfoGroup denied knowledge of the incident. Telephone Interview with Matthew Graves, Chief Data Officer, InfoGroup (Mar. 31, 2014).

Finally, I call for greater oversight of the data broker industry with the Fair Credit Reporting Act as a template for legislation. I argue that data brokers should ensure their lists are used for legitimate business needs, and should be held vicariously liable when their lists are misused. I conclude with a discussion of a potential Do Not Share list that would allow consumers to easily opt-out of data broker databases, as well as the need for greater education about the link between data collection and harmful scams.

II. TARGETING THE ELDERLY FOR FINANCIAL ABUSE: THE GRANDPARENT SCAM

Seniors across the US have been targeted for the grandparent scam—also known as the emergency scam—at unprecedented rates. The individual stories are disheartening. Grandparents in Fort Collins, Colorado wired $16,000 to help a woman they thought was their daughter caught in a Peruvian jail.[14] A Macon, Georgia woman sent thousands of dollars to an impersonator who said she was involved in a car crash and needed cash.[15] In Chicago, a grandmother of eleven and a great-grandmother of thirteen children was convinced that her

[14] *See* Laurie Cipriano, *Fort Collins Grandparents Scammed out of $16k*, THE COLORADOAN (Nov. 11, 2013), *available at* http://www.coloradoan.com/article/20131111/NEWS01/311110067/Fort-Collins-grandparents-scammed-out-16K.

[15] *See* Andres Lopez, *Macon Woman Victim of 'Grandparent Scam,'* MACON TELEGRAPH (Nov. 28, 2013), *available at* http://www.macon.com/2013/11/28/2803488/macon-woman-victim-of-grandparent.html.

granddaughter was locked up in a California jail with a broken nose, and wired a total of $35,000 in two installments.[16]

As part of the scam, a fraudster will call a senior pretending to be a family member or relative, perhaps because the scammer masked his identity on caller ID.[17] The criminal fakes an emergency—for instance, the loved one might have been jailed in a foreign country, mugged, or harmed in an accident.[18] Then they ask the grandparent for a wire transfer to cover expenses to help their loved one get home safely.[19] The scammer might feign shame that this emergency happened, and beg the grandparent for secrecy.[20] Oftentimes, they put pressure on the grandparent to wire money immediately.[21]

In 2009, the Federal Trade Commission received just 743 reports of the scam, but the scam has grown significantly, with 56,612 incidents reported between January 2010 and December 2013.[22] The crime rate is likely significantly higher,

---

[16] *See* Lisa Parker, *Scam Bilks Grandmother out of $35,000*, TARGET 5 NEWS CHICAGO (July 23, 2013), http://www.nbcchicago.com/investigations/target-5-lisa-parker-grandparents-scam-188000771.html.

[17] *See* Diane Lade, *AG Warns About New Technological Twist in 'Grandparent Scam,'* SUN SENTINEL (Apr. 4, 2011), http://articles.sun-sentinel.com/2011-04-04/business/fl-senior-scam-warning-20110404_1_grandparent-scam-con-artists-bondi.

[18] *See* Melanie Hicken, *Grandparent Scams Steal Thousands from Seniors*, CNN MONEY (May 22, 2013), http://money.cnn.com/2013/05/22/retirement/grandparent-scams/.

[19] *Id.*

[20] *Id.*

[21] *Family Emergency Scams*, FEDERAL TRADE COMM'N, http://www.consumer.ftc.gov/articles/0204-family-emergency-scams (last visited Apr. 2014).

[22] *See* FEDERAL TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY-DECEMBER 2013, at 82 (2014), available at

with authorities estimating that only 5% of victims report the scam.[23] Total losses from the scam are estimated to run into the tens of millions of dollars.[24] To make matters worse, police advise victims of cons that it is not likely that their money will be found and returned to them.[25] Police are in agreement that the grandparent scam can be traced back to scammers possessing detailed knowledge of their victim, whether from information garnered from lead lists purchased from data brokers, obituaries, or social media.[26] Fraudsters also recompile—for resale—lists of seniors who might have fallen for a past fraud or scam.[27] These lists sell for pennies per name, although some premium lists command much higher prices.[28]

A. Elderly Population as Vulnerable to Fraud

Older Americans are vulnerable to fraud schemes, especially given "(1) their availability, (2) their frailty, and (3) their financial resources."[29] Retired or homebound seniors are often available to answer when the phone rings, and telemarketers report that they are more likely to remain on the

---

https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2013.

[23] *See* Lea, *supra* note 4.

[24] *Id.*

[25] *Id.*

[26] *See Grandparent Scam Tips*, CONSUMER FEDERATION OF AMERICA, http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf (last visited Apr. 2014).

[27] *See* Moore, *supra* note 12, at 549–50.

[28] *Id.*

[29] Jeffrey Bratkiewicz, *"Here's a Quarter, Call Someone Who Cares"; Who is Answering the Elderly's Call for Protection from Telemarketing Fraud?*, 45 S.D. L. REV. 586, 588 (2000).

phone to hear a sales pitch.[30] Seniors may also feel isolated and lonely, especially if they live alone, far from friends or family, or without a recently deceased spouse.[31]

Frailty, real or perceived, increases elder vulnerabilities. A 2013 Wayne State University study, the first to look at predictors of financial victimization, found a 226 percent increase in fraud prevalence in elderly populations with high levels of depression and low social needs fulfillment.[32] Persons with undiagnosed early stages of dementia, which causes decreased cognitive functioning, may also be at greater risk of fraud susceptibility given their potentially increased difficulty in making rational choices.[33] The elderly are more often targeted for fraud than other groups, increasing their exposure to potential scams and resulting in more incidents of fraud.[34] By most accounts, there is at the very least a perception that the elderly are more trusting and less likely to perceive the dangers of exposing their personal information over the phone,[35] which emboldens scam artists.

---

[30] *See id.* at 589.
[31] *Id.*
[32] *See Psychological Vulnerable Older Adults are More Susceptible to Fraud*, SCIENCE DAILY (Apr. 25, 2013), http://www.sciencedaily.com/releases/2013/04/130425132441.htm.
[33] *See* Matthea Ross, *Why Are You Calling Me?: The Importance of the Do-Not-Call Registry in Protecting the Elderly from Financial Abuse*, 6 ALB. GOV'T L. REV. 663, 668 (2013).
[34] *See* Clarissa Cooper, *Professors' 3-Year Study Reveals Elderly are Most Targeted for Scams, but Not Vulnerable*, DOWNTOWN DEVIL (Dec. 12, 2013), http://downtowndevil.com/2013/12/12/52705/elder-scam-fraud-asu-research-study/; s*ee also Why Are the Elderly Being Targeted for Consumer Fraud and Scams?*, STETSON LAW (Feb. 11, 2013), http://www.stetson.edu/law/academics/elder/ecpp/media/update-why-the-elderly-02-11-2013.pdf.
[35] *See* Ross, *supra* note 33, at 666.

Meanwhile, scammers know that they can strike big when targeting the elderly. Households of adults aged 50 and over control 70 percent of the country's net worth,[36] and their numbers are growing. According to the US Census Bureau, the US population of adults 65 and older is rapidly growing especially as baby boomers retire, and it is expected to double from 39 million to 89 million by the year 2050.[37] By one estimate, more than 10,000 people are retiring every day.[38] With so many older adults living on fixed income or facing disabilities, finding a job is often not an alternative.[39] When scams cut into their savings, these victims might have no other choice but to turn to public assistance programs.[40]

Sentence enhancements aim to contemplate elder vulnerabilities and deter offenders. Federal Sentencing Guidelines enhance penalties for fraud targeting vulnerable victims[41] by two levels with a showing that the "defendant knew or should have known that a victim of the offense was a

---

[36] Johnny Parker, *Company Liability for a Life Insurance Agent's Financial Abuse of an Elderly Client*, 2007 MICH. ST. L. REV. 683, 684 (2007).

[37] Press Release, U.S. Census Bureau, Census Bureau Reports World's Older Population Projected to Triple by 2050 (June 23, 2009), http://www.census.gov/newsroom/releases/archives/international_population/cb09-97.html.

[38] *See* Parker, *supra* note 36, at 689 (quoting another source).

[39] *Id.*

[40] *Id.*

[41] The Commentary to the Federal Sentencing Guidelines defines a "vulnerable victim" as a person who, in part, "is unusually vulnerable due to age, physical or mental condition, or who is otherwise particularly susceptible to the criminal conduct." U.S. SENTENCING GUIDELINES MANUAL § 3A1.1 cmt n.2 (2010). The enhancement applies where the defendant "selected" the victim because of the vulnerability. *See* U.S. SENTENCING GUIDELINES MANUAL § 3A1.1.

vulnerable victim."[42] Two additional levels are added by showing "the offense involved a large number of vulnerable victims."[43] As evidence of targeting of the elderly, courts have considered lead lists. The Eighth Circuit surmised in *United States v. Whatley* that such lists provide "sufficient basis" for "application of the vulnerable-victim enhancement."[44]

B. "Trust, But Verify:" Current Education Efforts

A decentralized campaign to prevent the grandparent scam through education has had limited impact. Websites and office buildings post information bulletins warning seniors to verify emergency claims and to never wire money hastily.[45] Some suggest seniors develop a code word with relatives to ensure they can trust the person on the other end of the phone.[46] AARP informs its members about the dangers of the scam[47] and The Federal Trade Commission has posted a simple English and Spanish discussion of the dangers of these scams on its website.[48] Even Western Union has taken limited action, warning against making transfers to family members in unconfirmed emergency situations.[49]

---

[42] *Id.* § 3A1.1(b)(1).
[43] *Id.* § 3A1.1(b)(2).
[44] *United States v. Whatley*, 133 F.3d 601, 607 (8th Cir. 1998).
[45] *See, e.g.*, *Consumer Alert: Grandparents Scam*, ATT'Y GEN. OF THE ST. OF MICH., http://www.michigan.gov/ag/0,4534,7-164-18156-205169--,00.html (last visited Jan. 2014).
[46] *See* Alexandra Sellitto, *Campaign to Stop the Grandparent Scam*, ABC NEWS 7 N.Y. (Mar. 23, 2011), http://abclocal.go.com/wabc/story?section=news/local/new_jersey&id=8029905.
[47] *See* Kirchheimer, *supra* note 4.
[48] *See Family Emergency Scams*, *supra* note 21.
[49] Press Release, Western Union, Western Union & Better Business Bureau Partner to Protect Consumers from Emergency Scams (July 11, 2013), http://ir.westernunion.com/News/Press-Releases/Press-Release-

Despite these education efforts, the grandparent scam has continued to proliferate.[50] Right now, there are no studies to indicate just how many seniors hang up the phone when contacted as part of this scam. Research is needed in this area to determine the penetration of grandparent scam education efforts and to then target populations who might be less likely to have learned of the scam. Additionally, Western Union has not reported on the success or reach of its campaign to raise awareness of the scam, though media reports indicate that some shop clerks have talked seniors out of sending money by wire.[51] Education efforts will continue to have limited impact in this area, but this Note focuses instead on a different approach that proactively vets buyers of lead lists.

III. ENABLING THE SCAM: THE UNREGULATED DATA COLLECTION INDUSTRY

List making is the genius of a little-known but growing industry. The premise of the multi-billion dollar data broker industry is the ever-increasing demand for aggregated, accurate personal data for use in services such as marketing, authentication, directory listings, and reputation or eligibility

---

Details/2013/Western-Union--Better-Business-Bureau-Partner-to-Protect-Consumers-from-Emergency-Scams/default.aspx; *see also* Hicken, *supra* note 18.

[50] *See* FEDERAL TRADE COMM'N, *supra* note 22.

[51] As an anecdote, a woman in Vancouver Island, British Columbia had just wired $2,300 to her supposed grandson caught in a Montreal jail for drinking and driving when the shop clerk voided the transaction and revealed all: it was a scam. *See Grandparents Scam Foiled by Sharp Safeway Clerk*, CBC NEWS (Oct. 4, 2013), http://www.cbc.ca/news/canada/british-columbia/grandparents-scam-foiled-by-sharp-safeway-clerk-1.1912706.

screening. But unlike the credit reporting industry, the health care industry, and the financial industry, the data broker industry operates in a largely unregulated environment. The structure of the industry and the limited oversight it enjoys has benefited bad actors who can misuse the aggregated personal information.

A. The Data Industry

Buying, selling, renting, and trading data are common practices in today's economy.[52] Analytics companies, advertising networks, Internet Service Providers (ISPs), social networks, and data brokers all participate in acquiring and conveying data on the internet.[53] Marketing and survey firms,[54] grocery store loyalty programs,[55] and government agencies[56] collect data offline. Regulated entities, including Credit Reporting Agencies (CRA), medical groups, financial companies, and employers, also collect personal data.

---

[52] *See* Lois Beckett, *Everything We Know About what Data Brokers Know About You*, PROPUBLICA (June 13, 2014), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

[53] For a representative list of the types of companies that collect and share data, see the list developed by stakeholders as part of the NTIA Mobile Application Transparency process. *See Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*, NAT'L TELECOMM. & INFO. ADMIN. 3 (July 25, 2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

[54] *See* Bob Trebilcock, *Robbed By Phone*, GOOD HOUSEKEEPING, Jan. 1998, at 88.

[55] *See* Martin Bosworth, *Loyalty Cards: Reward or Threat?*, CONSUMER AFFAIRS (July 11, 2005), http://www.consumeraffairs.com/news04/2005/loyalty_cards.html (last visited June 24, 2015).

[56] *See* Logan Wayne, *The Data Broker Threat*, 102 J. CRIM. L. & CRIMINOLOGY 253, 263 (2012).

Data brokers are a subset of third party data collectors,[57] but data brokers are unique. They acquire personal information to aggregate it, package it, analyze it, and resell it at a profit without providing a consumer-facing service. Brokers maintain different types of products and services for diverse clients.[58] Marketing lists categorize individuals based on demographics, interests, or past purchase history. Directory listings aggregate personal information for use in people searches, reverse phone lookups, and white/yellow page listings. Authentication systems ensure that the right consumer is signing up for a given bank account or credit report. Finally, employers, banks, and creditors use reputation or eligibility screening systems to determine eligibility for a job, loan, or line of credit.[59]

The data these companies collect ranges from personally identifiable information to marketing characteristics

---

[57] Privacy Rights Clearinghouse maintains a listing of many known brokers; *see Online Data Vendors,* PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-information-brokers-list (last visited Apr. 2014). Major brokers include Acxiom, Epsilon, Equifax, Experian, Harte-Hanks, Intelius, Fair Isaac, Lexis Nexis, Markle, and Meredith Corp. *See* Natasha Singer, *Congress to Examine Data Sellers*, N.Y. TIMES, July 25, 2012, at B1, *available at* http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html. Online search services, many using the data garnered from these larger companies, include 1-800-US-Search, Address.com, Ancestry.com, InfoUSA, People Finder, Public Records Now, Spokeo, and WhitePages.com. Other brokers are smaller outfits without large corporate profiles.

[58] Acxiom describes these categories in its privacy policy. *See Acxiom's US Digital Advertising Products Privacy Policy*, ACXIOM, http://acxiom.com/about-acxiom/privacy/us-online-advertising-privacy-policy/ (last updated Sept. 24, 2013) [hereinafter *Acxiom Privacy Policy*].

[59] This final category is regulated under the Fair Credit Reporting Act (FCRA). *See infra* Part III.D.I.

to criminal background information. They offer searches that may reveal such personal information as full name, address, age, date of birth, phone number, relatives, and address history as well as specialized searches for criminal background and property record information. [60] Some brokers also have access to information that indicates purchase and transaction information, automobile purchases, health conditions, social media activity, and credit card information.[61]

When aggregating personal information into marketing lists, brokers develop demographic or interest-based classifications to group consumers.[62] For instance, a list might include all elderly people in a specific city or identify individuals as "Christian donors," "Proven Patriots," or "Hooked on Plastic."[63] The categories can get extremely sensitive and specific, as Consumer Advocate Pam Dixon pointed out at a December 2013 hearing of the Senate Committee on Commerce, Science, and Transportation.[64] Dixon pointed to categories such as "Police Officers and

---

[60] *See e.g.*, *24-Hour People Search Pass*, INTELIUS, https://intelius.com/24-hour.html, (last visited June 2015).

[61] *See* STAFF REP. FOR CHAIRMAN ROCKEFELLER, OFFICE OF OVERSIGHT & INVESTIGATIONS: MAJORITY STAFF, S. COMM. ON COMMERCE, SCI., & TRANSP., A REVIEW OF THE DATA BROKER INDUSTRY 13–14 (Dec. 18, 2013) [hereinafter COMMERCE REPORT], *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a.

[62] *What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Commerce, Sci., & Trans.*, 113th Cong. (2013) (statement of Pam Dixon, Exec. Dir., World Privacy Forum), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=e290bd4e-66e4-42ad-94c5-fcd4f9987781 [hereinafter Dixon].

[63] *Your Privacy For Sale*, CONSUMER REPORTS 41, 42 (Oct. 2006).

[64] *See* Dixon, *supra* note 62.

Troopers at Home," "Rape Sufferers," "Genetic Diseases Sufferers," "Dementia Sufferers," and "Addictive Behaviors, Alcohol and Drugs."[65]

Larger brokers like Acxiom maintain that they keep data for more sensitive purposes in separate databases with different levels of access restrictions enforced by contractual agreements with list users.[66] For instance, social security numbers would not be as readily available to purchasers of marketing lists.[67] These policies have evolved, especially after industry scrutiny in the aftermath of data leaks. In 2004, now defunct ChoicePoint, a major data broker acquired by LexisNexis in 2008,[68] revealed it had sold personal information including Social Security numbers of some 145,000 people to Nigerian criminals posing as representatives of legitimate businesses.[69] ChoicePoint apologized, saying it had failed to properly vet the companies.[70]

In comparison to social security numbers, brokers put fewer restrictions on access to marketing lists.[71] Take for example LeadsPlease, a website that touts its ability to provide

---

[65] *Id.*
[66] *See Acxiom Privacy Policy*, *supra* note 58.
[67] *See id.*
[68] *See* Toby Anderson, *LexisNexis Owner Reed Elsevier Buys ChoicePoint*, USA TODAY (updated Feb. 21, 2008), *available at* http://usatoday30.usatoday.com/money/industries/2008-02-21-reed-choicepoint_N.htm.
[69] *See* Tom Zeller, *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES (Feb. 24, 2005), *available at* http://www.nytimes.com/2005/02/24/business/24datas.html.
[70] *See* Chris Noon, *Smith: ChoicePoint CEO Apologizes Profusely for Security Breaches*, FORBES (Mar. 16, 2005), *available at* http://www.forbes.com/2005/03/16/0316autofacescan02.html.
[71] *See, e.g.*, *Acxiom Privacy Policy*, *supra* note 58.

lists of no less than 1,000 names within minutes.[72] Personal data on that site can be sorted based on category and purchased for six cents per name.[73] Those names, in turn, were purchased from LeadsPlease's partner, data broker giant Experian.[74]

B. Sources of Personal Information

Data brokers through the years have amassed troves of names, to the point that Acxiom boasts a database of 500 million people worldwide[75], including "nearly every Internet user in the U.S."[76] Before technology brought this information into one central database, the information was decentralized, in city hall filing cabinets, in telephone white pages, and in individual company or retailer databases. Brokers have purchased and amassed this data over time from disparate sources, which the Government Accountability Office (GAO) sorts into three categories: public records, nonpublic information, and publicly available information.[77]

---

[72] *See* LEADSPLEASE, http://leadsplease.com (last visited Apr. 2014).
[73] *See id.*
[74] *See Data Quality*, LEADSPLEASE, http://www.leadsplease.com/data_quality (last visited Apr. 2014).
[75] *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.
[76] *See Q1 FY14 Earnings Conference Call Script*, ACXIOM, (July 31, 2013) (quoting Scott Howe, Chief Exec. Officer, Acxiom) http://d3u9yejw7h244g.cloudfront.net/wpcontent/uploads/2013/09/FY14_Q1_Earnings_Prepared_Remarks-Final.pdf.
[77] *See GAO Report*, *supra* note 8, at 3.

1. Data Acquired from Public Records

A primary source for data is "bulk data purchases" from government agencies.[78] Many local agencies make considerable sums of money from selling public records.[79] Criminal records make up the majority of these bulk data purchases. Other records include census data, property records, DMV records, voter registrations, and marriage and death certificates.[80] While some localities have placed statutory limitations on permissible uses of government records,[81] most do not place restrictions on the data they sell.[82]

2. Nonpublic Information

Data brokers seek out additional sources of personal information from nonpublic records. When an individual fills out a survey in a restaurant, the survey company that aggregates the data could then sell it to a data broker.[83] When a consumer signs up for a loyalty card at a grocery store,

---

[78] *See* Wayne, *supra* note 56, at 263.

[79] *See id.* at 263–64. State laws vary with regard to selling records, though most are permissive in allowing bulk data purchases. *See* SEARCH, NAT'L CONSORTIUM FOR JUST. INFO. & STAT., REPORT OF THE NATIONAL TASK FORCE ON THE COMMERCIAL SALE OF CRIMINAL JUSTICE RECORD INFORMATION 39-43 (2005), *available at* http://www.search.org/files/pdf/RNTFCSCJRI.pdf.

[80] *See Commerce Report*, *supra* note 61, at 15; *GAO Report*, *supra* note 8, at 4.

[81] *See, e.g.*, CAL. GOV'T. CODE § 6254(f)(3) (West 2014); *see also* L.A. Police Dep't v. United Reporting Pub. Corp., 528 U.S. 32 (1999) (upholding on First Amendment grounds a California statute restricting access to court records to those requesting the records for one of five given purposes, which cannot include marketing).

[82] *See* SEARCH, *supra* note 79.

[83] *See* Trebilcock, *supra* note 54.

personal information supplied and shopping history can then be sold and added to a consumer's data broker profile.[84] Other times, companies partner with brokers to enhance their lists[85] or to exchange their lists for additional lists of marketing prospects.[86]

Reports indicate that some brokers have used nonpublic information without permission.[87] In some instances investigated by Senator John Rockefeller's staff on the Committee on Commerce, Science, and Transportation, Acxiom labeled companies it did business with as sources of data, when in fact the companies merely thought they were purchasing Acxiom's products, not contributing to the company's databases.[88] Also, in 2010, the *Wall Street Journal* released a report that showed third-party applications on Facebook had sold personal data collected from users to data brokers, including data from users "who set their profiles to Facebook's strictest privacy settings."[89] In response, Facebook put various applications on probation and made technical changes to restrict information in the future, but that stolen

---

[84] *See* Bosworth, *supra* note 56.
[85] *See Commerce Report*, *supra* note 61, at 21.
[86] *See id.*, at 17–18.
[87] Perhaps the most egregious form of gathering personal data that some data brokers once used, pretexting, is now prohibited. *See* Terry Collins, *Hewlett-Packard 'Pretexting' Scandal Leads to Private Investigators' Sentencing in San Jose*, ASSOCIATED PRESS (July 13, 2012), http://www.mercurynews.com/business/ci_21061358/hewlett-packard-pretexting-scandal-leads-private-investigators-sentencing.
[88] *See Commerce Report*, *supra* note 61, at 20.
[89] Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach: Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds*, WALL ST. J. (Oct. 17, 2010), *available at* http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

information might still be included in some data broker databases.[90]

3. Publicly Available Information

Other sources of information that data brokers use to develop their databases include telephone and business directories, printed materials, and records posted online.[91] Some brokers might sift through online data to incorporate the information into their proprietary profiles of individuals.[92]

C. Beyond Lead List Scams: Additional Harms of Data Broker Products

Lead lists are not the only product that data brokers sell. Their individual reference services enable web users to search for contact information for friends, neighbors, or even long-lost relatives.[93] Their authentication services keep credit reports and banking systems safe.[94] Their marketing data helps large and small businesses alike determine how to best market their products and services.[95] The troubling aspect of the industry, however, has less to do with the nature of its products and more to do with consumer relations.

---

[90] *See* Mike Vernal, *An Update on Facebook UIDs*, FACEBOOK DEVELOPER BLOG (Oct. 29, 2010), https://developers.facebook.com/blog/post/422/.
[91] *See GAO Report*, *supra* note 8, at 4.
[92] *See Commerce Report*, *supra* note 61, at 21.
[93] *See, e.g.*, *Acxiom Privacy Policy*, *supra* note 58.
[94] *See id*.
[95] *See id*.

Individual consumers rarely interface with data brokers directly, and have very little insight into the industry's practices.[96] As a result, brokers' economic loyalties lie with other businesses, not consumers who barely know that these companies exist. Larger brokers might face public scrutiny from a data breach or from selling lists to scammers, but the majority of obscure brokers have almost no economic incentives to appease consumer concerns or guard consumer identities. Perhaps as a result, the model of selling personal information for profit has time and again run up against the realities of potential abuse. In particular, broker data can be harmful when inaccurate, when used for identity theft or stalking, and when used to target vulnerable populations. This section reviews all of these known harms to demonstrate that broker oversight can result in multiple beneficial outcomes.

1. Reputational Harms from Inaccurate Data

When reporter Bob Sullivan of MSNBC requested his "background search" report from Intelius in 2006, he was surprised to learn he had been convicted of child molestation.[97] He also learned that he was associated with one Shawn Sullivan, an individual convicted of manslaughter. "Let me assure you, neither is true," Sullivan wrote.[98] "There's Bob Sullivan, the Red Tape Chronicles author. Then there's Bob Sullivan, who might be a bankrupt child molester with a brother who's a killer. … If perception takes on its own reality, certainly a computer creation can, too."[99] Reputational harm

---

[96] *See GAO Report*, *supra* note 8, at 4.
[97] *See* Bob Sullivan, *Bob the Writer, Bob the Molester*, NBC NEWS (May 3, 2006), http://redtape.nbcnews.com/_news/2006/05/03/6346099-bob-the-writer-bob-the-molester.
[98] *Id*.
[99] *Id*.

can arise easily from such inaccurate information. Anyone who ran a check on Sullivan might in fact think he was a child molester. This is unfair both to Sullivan and to the consumer who paid $50 for the report. Of course, top brokers continue to perfect their algorithms and data collection to increase the value of their services.

2. Identity Theft

Identity thieves are attracted to data brokers given the vast data that they store, including credit histories, payment card data, and social security numbers. In a recent example, identity theft website Superget.info simply purchased sensitive personal data from an Experian affiliate[100] and then sold the records of more than 500,000 people.[101] In a similar scheme, identity theft website, SSNDOB, hacked into LexisNexis and two other brokers to collect personally identifiable information that included the social security numbers of public figures like Beyoncé, First Lady Michelle Obama, and former FBI Director Robert Mueller.[102] SSNDOB data sold for 50 cents to $2.50 per record.[103] Experian and LexisNexis have not clarified whether they are taking action to secure their files against repeat offenders.

---

[100] *See* Brian Krebs, *Experian Sold Consumer Data to ID Theft Service*, KREBS ON SECURITY (Oct. 20, 2013), http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

[101] *See* Dan Goodin, *Can We Trust the Data Brokers Who Store Our Most Intimate Private Details?*, ARS TECHNICA (Oct. 21, 2013), http://arstechnica.com/security/2013/10/can-we-trust-the-data-brokers-who-store-our-most-intimate-private-details/.

[102] *See* Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KREBS ON SECURITY (Sept. 25, 2013), http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

[103] *See id.*

3. Facilitation of Stalking

Individual reference services provided by data brokers can assist stalkers in targeting a victim. While some victims of stalking are able to enroll in Address Confidentiality Programs (ACPs) in 36 states to mask their actual residential addresses,[104] data brokers in most states are under no legal obligation to omit ACP data in their databases. One exception is California, which enacted the Internet Disclosure Prohibition in 2011, making it illegal for data brokers to include ACP data in their directories after receiving written requests to remove the information.[105] Indiana passed a weaker law in 2013 that does not place requirements on brokers, but allows victims of domestic violence and law enforcement officers to restrict the inclusion of their home address in government database websites.[106]

In at least one state, the courts have found liability for selling personal data used in stalking.[107] In the New Hampshire case of *Remsburg v. Docusearch, Inc.*, a man paid data broker Docusearch $20 for the birth date of Amy Lynn Boyer, his stalking victim, and $45 for her social security number.[108] He then paid to obtain her employment records and her home address, and he eventually used the information to

---

[104] *Address Confidentiality Programs*, STALKING RESOURCE CENTER, http://www.victimsofcrime.org/our-programs/stalking-resource-center/help-for-victims/address-confidentiality-programs (last visited Apr. 2014).
[105] *Personal Information: Internet Disclosure Prohibition*, S.B. 636, 2011 S., 2011–2012 Sess. (Cal. 2011).
[106] *Privacy of Home Addresses*, H.B. 1219, 118th Gen. Assemb., 1st Reg. Sess. (Ind. 2013).
[107] *See* Remsburg v. Docusearch, Inc., 149 N.H. 148 (2003).
[108] *See id.* at 152–53.

track Boyer and murder her.[109] In considering the liability of Docusearch, the New Hampshire Supreme Court found an affirmative duty to exercise reasonable care in disclosing personal information that could be used illegally for stalking or identity theft.[110] In particular, the court deemed "foreseeable" the potential illegal stalking: "The risk of criminal misconduct is sufficiently foreseeable so that a [data broker] has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[111]

4. Abusive Marketing

The potential for abusive marketing practices and consumer scoring is a final major harm brought to light by a December 2013 report of the Senate Committee on Commerce, Science, and Transportation.[112] A data broker might score consumers, for instance, to determine if they are eligible for special offers.[113] But armed with detailed personal information, the broker might use a consumer's financial situation or health condition to perfect that score, targeting consumers who would be likely to accept the offer.[114] Some companies might use the information to price discriminate in their offers to consumers, while retailers might discriminate by devoting greater sales attention to shoppers with higher incomes or spontaneous purchasing habits.[115] The Senate Committee report demonstrates that personal information can be abused for financial gain, not just by scam artists but also by

---

[109] *See id.*
[110] *See id.* at 154–55.
[111] *Id.* at 155.
[112] *See generally Commerce Report*, *supra* note 61.
[113] *See id.* at 8.
[114] *See id.* at 13–14, 24.
[115] *See id.* at 7.

retailers, financial institutions, and companies with services to sell.

D. Laws Governing Data Accumulation and Resale

Despite the potential for data broker information to harm consumers, Congress has never implemented blanket, baseline privacy legislation, instead opting for targeted legislation that controls the collection of sensitive data collected from various industries. These laws serve as a template for legislative action that aims to protect data broker databases from misuse.

1. Fair Credit Reporting Act (FCRA)

The statute with most reach into the data collection landscape is the Fair Credit Reporting Act (FCRA), first enacted in 1970 and most recently amended in 2010 by the Dodd-Frank Act.[116] The FCRA regulates profiles much like those held by data brokers, except that the profiles relate to credit histories specifically. The bill's writers were concerned that inaccuracies would lead to denial of credit—necessary for a loan but also relied upon by employers, realtors and landlords, and banks of all kind.[117] Originally in the 1960s, there were few rules about who could access consumer credit reports or what they could include. Privacy scholars like Columbia Law School Professor Alan Westin were concerned that a lack of regulation would result in new erosions of

---

[116] 15 U.S.C. §§ 1681–1681x (2013).

[117] *See* Marc Roth and Charles Washburn, *Data Brokers Face Blurring Lines, Increased Regulatory Risks*, BLOOMBERG L. (Aug. 22, 2012), http://www.bna.com/data-brokers-face-blurring-lines/.

personal privacy: "I would suggest that it is true that we are building a national private intelligence system."[118]

The FCRA brought greater consumer protections, focusing not on the collection of data but on ensuring that consumer reporting agencies were responsible when compiling and disclosing their records. The law allows consumers to dispute and correct inaccurate information[119] and requires consumer reporting agencies to ensure the "maximum possible accuracy" of personal information.[120] But the FCRA applies only to "consumer reporting agencies" that provide "consumer reports."[121] Only a agency is a consumer report; the statute does not cover other reports, such as a data broker report used for marketing purposes.[122]

---

[118] *Fair Credit Reporting: Hearings Before the S. Subcomm. on Financial Institutions, Comm. on Banking and Currency*, 91st Cong. 79 (1969) [hereinafter *Fair Credit Reporting Hearings*], *available at* http://congressional.proquest.com/congressional/docview/t29.d30.hrg-1969-bcs-0025?accountid=14678.

[119] 15 U.S.C. § 1681i(a)–(d) (2013).

[120] 15 U.S.C. § 1681e(b).

[121] 15 U.S.C. § 1681a(d) (A consumer report is a "communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, … character, general reputation, personal characteristics, or mode of living which is used … as a factor in establishing the consumer's eligibility for-- (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes" or other specified purposes.); 15 U.S.C. § 1681a(f) (A consumer reporting agency "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.").

[122] *See* Mirfasihi v. Fleet Mortg. Corp., 551 F.3d 682 (7th Cir. 2008) (finding personal information that defendant corporation shared was not a consumer report because the company was not a consumer reporting agency).

The FCRA limits the availability of consumer reports to instances when the CRA "has reason to believe" the person receiving the report:

"(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished …; or

"(B) intends to use the information for employment purposes; or
"(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or …

"(F) otherwise has a legitimate business need for the information (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the account."[123]

Here, the FCRA specifically cites use of an individual's credit information as permissible in extension of credit, for purposes of employment or insurance, or for a legitimate business need. Congress did not, however, intend legitimate business needs to be limitless. Using information for a lawsuit defense or to learn about a job applicant's spouse are some examples that courts have determined to be outside legitimate needs.[124] The FCRA also placed limits on the use and reuse of individual credit data. Users of the data must report to a consumer if they take "adverse action" against a consumer's interests, such as denying employment or credit based on an

[123] 15 U.S.C. § 1681b(a)(3) (2013).
[124] Michael L. Matula, *Be Careful, the FCRA Might Apply to You*, 19 PREVENTATIVE L. REP. 26 (2000–2001).

individual's credit report contents.[125] Credit reporting agencies must allow consumers to opt out of information sharing with third parties for prescreened marketing offers.[126] Consumer reports are protected from access under false pretenses, including a potential $5,000 fine and misdemeanor prison sentence.[127]

2. Gramm-Leach-Bliley Act (GLBA)

Another law that regulates information disclosure by data brokers is the Gramm-Leach-Bliley Act (GLBA). Enacted in 1999, the law restricts disclosure of nonpublic personal information by a financial institution without first notifying consumers and providing them with an opportunity to opt-out, subject to exceptions.[128] Third parties like data brokers that receive nonpublic personal information from a financial institution face restrictions on reuse and redisclosure of the data, even if they are not financial institutions themselves.[129] In cases where a data broker obtains personal information from a bank to process a transaction or run the name against its proprietary database to protect against fraud, that information may not be reused or redisclosed for marketing purposes.[130]

3. Driver Privacy Protection Act (DPPA)

A third federal law, the Driver Privacy Protection Act (DPPA), restricts data broker access to motor vehicle records

---

[125] 15 U.S.C. § 1681m(a)(1) (2013).
[126] 15 U.S.C. § 1681b(e).
[127] 15 U.S.C. § 1681q.
[128] 15 U.S.C. § 6802(a)–(b).
[129] 15 U.S.C. § 6802(c) (2013).
[130] *See Commerce Report*, *supra* note 61 at Appendix I, p.3; *GAO Report*, *supra* note 8, at 9.

and provides a template for protection of sensitive information contained in government files. The law prohibits state motor vehicle departments from sharing personal information obtained from drivers without consent of the individual, with limited exceptions.[131] The Second Circuit has found a duty on the part of data brokers to exercise reasonable care before disclosing personal information they may have obtained from a motor vehicle department.[132] As the Second Circuit Court of Appeals wrote, "Given the nature of information available through motor vehicle records—e.g., social security number, medical or disability information, and home address—the DPPA's purpose would be severely undermined if resellers' disclosures were not subject to a duty of reasonable inquiry."[133]

Taken together, these three laws restrict data brokers from selling services that bear on credit or employment determinations, that make available nonpublic financial information of consumers, and that are derived from motor vehicle records. But these laws do not govern data broker databases sold for marketing purposes. This loophole makes it easier for scam artists to purchase lead lists, access sensitive personal information, and target victims.

E. Current Oversight Mechanisms

No single governmental entity or law covers enough of the data broker problem to be wholly responsible for

---

[131] 18 U.S.C. § 2721 (2013).
[132] *See* Gordon v. Softech Int'l, Inc., 726 F.3d 42, 56 (2d Cir. 2013) (finding "inconceivable" that a drop down menu of possible permissible uses for personal information regulated under DPPA was a strong enough protection for the personal information or deterrent against improper use or disclosure, thus violating the Act).
[133] *Id.* at 56.

enforcement of privacy and anti-fraud provisions. The Federal Trade Commission and Senate Committee on Commerce, Science, and Transportation have filled the regulatory and legislative gap in oversight through hearings and reports on the industry. As the industry has matured, it has generally structured its services to comply with the Fair Credit Reporting Act and to adhere to guidance published by the Federal Trade Commission.

1. Regulatory Gap Filling

The Federal Trade Commission (FTC) is the de facto regulator of the data broker industry given the FTC's expertise acquired through enforcement of the FCRA and other privacy laws. In May 2014, the FTC released the report "Data Brokers: A Call for Transparency and Accountability,"[134] where the agency called on Congress to mandate greater opportunities for consumers to access and correct their data and opt-out of data collection.[135] A proposed centralized industry portal would help consumers learn about the data collection process and access opt-out links.[136]

The report was more muted on the topic of oversight of list users. Instead of legislation, the report called on the industry to adopt various best practices that included the requirement to "conduct due diligence to ensure that data … is not used to deny consumers credit, insurance, employment, or

---

[134] *See* FEDERAL TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), http://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.
[135] *See id.* at 49–53.
[136] *See id.* at 50–51.

the like."[137] Commissioner Julie Brill disagreed in her concurrence appended to the report. Writing that "[d]ata brokers are well-situated to monitor their clients' data use and to be part of an early warning system when their highly sensitive information is used for unlawful purposes," Commissioner Brill called for legislation that would require brokers to ensure their products were not used for unlawful purposes.[138] Since the report's release, no legislative action has implemented the FTC's proposals.

Despite a lack of statutory oversight of brokers, the FTC has taken limited Fair Credit Reporting Act enforcement action against data brokers that developed and sold regulated consumer reports. In particular, the FTC charged online data broker Spokeo with violating the FCRA because of Spokeo's use of the tagline, "Explore Beyond the Resume."[139] The suggestion, according to the FTC, was that the service could be used as an employment background check.[140] Spokeo did not follow the FCRA's requirements, including ensuring the information it provided was used for legitimate business purposes and providing consumers with the opportunity to correct their profiles.[141] As a result of the scrutiny, the FTC

---

[137] *Id.* at 56.
[138] *Id.* at C-7.
[139] *See* Bob Sullivan, *FYI EVERYONE: Spokeo Fined, but It's Still Really Spooky*, NBC NEWS (Jun. 13, 2012), http://redtape.msnbc.msn.com/_news/2012/06/13/12204386-fyi-everyone-spokeo-fined-but-its-still-really-spooky?lite.
[140] *See id.*
[141] *See* Press Release, Federal Trade Comm'n, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (Jun. 12, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

and Spokeo settled for $800,000 in 2012, and Spokeo no longer markets itself to employers as a supplier of employee background checks.[142] Despite the win, the lesson for the data broker industry was one of marketing rather than protecting personal information. Had Spokeo marketed itself as an individual reference service rather than as a service for employers, the case might never have merited scrutiny under the FCRA.

The FTC has also pursued users of consumer reports for failure to follow the FCRA's rules. The FTC brought suit against a mobile application company, Filiquarian Publishing LLC, for providing criminal background checks to users on its mobile app with data it purchased from Choice Level LLC.[143] The app in fact disclaimed liability under the FCRA by saying it was not to be considered a "consumer reporting agency," but the FTC said that this disclaimer was not enough if the company was not monitoring access for permitted uses.[144]

2. Self Regulation

The industry has proven time and again that it is unwilling to develop a strong self-regulatory regime. Major data brokers today are represented as part of the Direct Marketing Association (DMA), the industry association that

---

[142] *See* Chloe Albanesius, *Spokeo Fined $800,000 for Deceptive Web Profiles*, PC MAGAZINE (Jun. 12, 2012), http://www.pcmag.com/article2/0,2817,2405729,00.asp.

[143] *See* Press Release, Federal Trade Comm'n, Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), http://www.ftc.gov/news-events/press-releases/2013/01/marketers-criminal-background-screening-reportsto-settle-ftc.

[144] *See id.*

has fought against government action to regulate data brokers.[145] DMA released research stating restrictions on data broker activity could cost the economy $110 billion in revenue.[146] The Association has also vigorously defended its self-regulatory guidelines, asserting that marketing lists that are not used to make eligibility determinations (similar to the "adverse action" clause of the Fair Credit Reporting Act) should not be subject to regulation.[147] DMA says it requires its members to notify consumers of their collection practice policies and to provide an opportunity to opt-out.[148] DMA also encourages marketing lists to be shared only with reputable users.[149] DMA ethics guidelines provide that data brokers sharing data on children, older adults, health care or treatment, account numbers, or financial transactions "should"[150] review promotional materials to "ensure that their customers' use of

---

[145] *See generally* Press Release, Direct Mktg. Ass'n, FTC 'Data Broker' Investigation Will Highlight Invaluable Benefits of Data-Driven Marketing to Consumers and Economy (Dec. 18, 2012), http://www.dmaresponsibility.org/cgi/disppressrelease?article=1566; *DMA: Rockefeller's Proposed Data Law Would Make Info Less Secure*, ADAGE (Feb. 13, 2014), http://adage.com/article/privacy-and-regulation/dma-rockefeller-s-data-law-make-info-secure/291702/.

[146] See Katy Bachman, *Big Data Added $156 Billion in Revenue to Economy Last Year*, ADWEEK (Oct. 14, 2013), http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107.

[147] *See* Rachel Thomas, *Data Brokers Under Fresh Attack from Congress*, DIRECT MKTG. ASS'N (Feb. 14, 2014), http://thedma.org/advance/data-driven-marketing-ideas/data-broker-under-fresh-attack-from-congress-dma-leading-the-fight/.

[148] *See* DIRECT MKTG. ASS'N, GUIDELINES FOR ETHICAL PRACTICE 25 (2014), http://thedma.org/wp-content/uploads/DMA_Guidelines_January_2014.pdf.

[149] *Id.*

[150] Various other articles make use of the imperatives "must" and "shall" in contrast to this article. *Id.*

the data is both appropriate and in accordance with their stated purpose."[151]

To enforce these provisions, DMA states that it reviews consumer complaints, works with companies to correct non-compliance, publicly shames members who refuse to alter their activities, and refers non-members found in violation of the ethics guidelines to law enforcement.[152] Still, these principles do not specify exactly how brokers should vet list users or specify the consequences for not doing so. The guidelines have not required point of disclosure notification to consumers that their information might be sold to third parties, and the rules have not mandated consumer friendly opt-out procedures. DMA treats social security numbers and credit card numbers sensitively, but does not treat birthdates or telephone numbers with elevated sensitivity.[153] The guidelines also do not discuss individual consumer recourse or legal sanctions for misuse of data.

Previously, data brokers developed their own self-regulatory association, although it disbanded in the early 2000s. In 1997, fourteen major data brokers released self-regulatory principles as part of a new industry group, the Individual Reference Services Group (IRSG).[154] IRSG committed to not display SSNs or dates of birth in products

---

[151] *Id.* at 25–26 (Article #36).
[152] DIRECT MKTG. ASS'N, DMA REPORT ON ETHICS COMMITTEE FINDINGS, http://www.dmaresponsibility.org/CaseReport/ (last visited Apr. 2014).
[153] *See* DIRECT MKTG. ASS'N, *supra* note 148, at 22 (Article #32).
[154] *See Internet Privacy: Hearing Before the Subcomm. on Courts and Intell. Prop., H. Comm. on the Judiciary*, 105th Cong. 11 (Mar. 26, 1998) (statement of the Federal Trade Comm'n), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-privacy/privacy.pdf.

distributed publicly and also agreed to truncate the information when sold to commercial buyers.[155] The industry said it would acquire information from reputable sources, restrict certain types of information, and provide copies of individuals' files on request.[156] The industry even agreed to enforcement measures, including legal sanctions if industry members did not follow the principles.[157] Measured against today's DMA guidelines, these ideas were radical. But IRSG did not last. The industry made the case, after the passage of the Gramm-Leach-Bliley Act, that self-regulation was no longer necessary, even though GLBA regulates financial institutions—not commercial data brokers —and would not bring the same protections as IRSG.[158]

In the aftermath of the IRSG, some brokers have joined DMA, but they are subject to few other external pressures. Recently, news reports in *The New York Times* that spotlighted Acxiom[159] for its slow response to consumer opt-out requests[160] acted to pressure the company into developing a

---

[155] *See Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers: Before the Subcomm. on Social Security, H. Comm. on Ways & Means*, 107th Cong. 112 (May 22, 2001) (statement of Ronald Plesser, Coordinator, Individual Reference Services Grp.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-107hhrg74226/pdf/CHRG-107hhrg74226.pdf.

[156] *See id.* at 112.

[157] *See id.*

[158] INDIVIDUAL REFERENCE SERVICE GRP., NOTICE OF TERMINATION OF IRSG, http://web.archive.org/web/20021013091209/http://www.irsg.org/html/termination.htm (last visited Apr. 2014).

[159] *See* Natasha Singer, *You for Sale*, N.Y. TIMES, Jun. 17, 2012, at BU1 *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[160] *See* Natasha Singer, *Consumer Data, but Not for Consumers*, N.Y. TIMES, July 22, 2012, at BU3, *available at* http://www.nytimes.com/

new website to give consumers added control over the marketing of their data.[161] Despite empowering consumers, the site has faced criticism from public advocates for requiring extensive personal data to sign up, for limiting the data consumers can see, and for weak opt-out options.[162] One commenter questioned whether the system was designed to collect more data from consumers to augment the Acxiom database.[163] Self-regulation has thus not dispelled criticisms or prevented leakage of broker lists for untoward purposes.

3. Legislation

While data brokers have faced unprecedented scrutiny, proposed legislative solutions are not sufficient to protect consumers from scams enabled by data broker products. Following the Government Accountability Office report identifying the need for legislative action[164] and the Committee on Commerce, Science, and Transportation report that detailed various harms of marketing products,[165] Senators John Rockefeller and Edward Markey introduced data broker-specific proposals for reform with the February 2014 Data

---

2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html.

[161] *See* Natasha Singer, *Acxiom Lets Consumers See Data It Collects*, N.Y. TIMES, Sept. 5, 2013, at B6, *available at* http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html.

[162] *See id.*

[163] Natasha Singer, *Getting a Glimpse of your own marketing data online*, N.Y. TIMES (Sept. 4, 2013), http://bits.blogs.nytimes.com/2013/09/04/getting-a-glimpse-of-your-own-marketing-data/ (quoting Ashkan Soltani).

[164] *See GAO Report*, *supra* note 8.

[165] *See Commerce Report*, *supra* note 61.

Broker Accountability and Transparency Act (DATA).[166] The legislation, which was reintroduced by Senators Markey, Blumenthal, Whitehouse, and Franken in 2015,[167] recognizes data broker databases as sensitive and requires brokers to establish procedures to ensure their records are accurate, provide consumers with access to review their personal information at least once per year for free, provide a dispute resolution process to correct inaccuracies, and permit consumers to opt out from marketing lists. The legislation proposes civil penalties on data brokers and grants the FTC oversight and enforcement authority, while preserving the authority of state attorneys general to take action against brokers.[168]

The bill does not, however, address one of the major concerns of the Senate Committee's report: abusive marketing tactics.[169] DMA has criticized the breadth of the definition in the bill of "data broker,"[170] arguing marketers "are all data brokers now."[171] The new data broker legislation is similar to past proposals from Senator Patrick Leahy, last introduced in

---

[166] *See* Data Broker Accountability and Transparency Act of 2014, S. 2024, 113th Cong. (2014) [hereinafter DATA Act].
[167] *See* Data Broker Accountability and Transparency Act of 2015, S. 668, 114th Cong. (2015).
[168] *See id.*
[169] *See Commerce Report*, *supra* note 61.
[170] The DATA Act defines a data broker as a "commercial entity that collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell the information or provide third party access to the information," *supra* note 166.
[171] Rachel Thomas, *Data Brokers Under Fresh Attack from Congress*, DIRECT MKTG. ASS'N (Feb. 14, 2014), http://thedma.org/advance/data-driven-marketing-ideas/data-broker-under-fresh-attack-from-congress-dma-leading-the-fight/.

the 111th Congress as part of the Personal Data Privacy and Security Act of 2009.[172] That legislation, which was reported out of the Judiciary Committee, would have similarly required brokers to disclose the information they have collected and allow correction of inaccuracies.[173] In their minority response to the bill, Senators Jeff Sessions and John Kyl disagreed with the intent of the bill.[174] Calling the legislation "far too broad," they wrote that the new rules could perversely apply to entities that use broker data for authentication or fraud prevention.[175] The Senators also cautioned against provisions that would make it more difficult for law enforcement to make use of broker services, citing an audit by the GAO that found that ninety-one percent of broker information was used by law enforcement or counterterrorism agencies.[176]

Any legislative initiative could face First Amendment challenges to restrictions on commercial speech, as seen in state-level cases. When Washington State prohibited the release of addresses, phone numbers, and other personal data of police officers and court employees, a website operator challenged the statute. Even though the law applied only to publishing the information with intent to harm or intimidate, the Court for the Western District of Washington found, in *Sheehan v. Gregoire*, that the statute impeded protected speech and did not serve a compelling state interest.[177] This contrasts

---

[172] *See* Personal Data Privacy and Security Act of 2009, S.1490, 111th Cong. (2009).
[173] *See id.*
[174] *See* S. REP. NO. 111–110, at 25–28 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-111srpt110/pdf/CRPT-111srpt110.pdf.
[175] *Id.*
[176] *See id.*
[177] *See* Sheehan v. Gregoire, 272 F. Supp. 2d 1135 (W.D. Wash. 2003).

with consistent judicial findings that the Fair Credit Reporting Act regulates commercial speech outside the protection of the First Amendment.[178] The contrast acts as a reminder that legislation must serve a compelling interest in order not to be subjected to strict scrutiny.

IV. MANDATE DATA BROKER VETTING AND STRENGTHEN CONSUMER OVERSIGHT OF DATA

Despite the current legal and regulatory framework, data broker lists proliferate, and grandparent scams persist. Nearly a decade since the data broker industry promised to self-regulate, their files are porous and few maintain a public profile. Consumers cannot easily opt-out or view the information held about them or have confidence that their personal information is sold to a reputable end-user. Meanwhile, media reports have emphasized to the elderly the dangers of picking up the phone and wiring money,[179] but the scam persists. The rewards are great, and the risks of getting caught are low. Armed with valuable leads purchased from a data broker, determining whom to call is too easy.

Consumers should not have to worry that their profile might be used against them or think about the need to opt-in or opt-out. Data brokers should guard this information by design. They should carefully vet the companies receiving their information and face consequences for misuse. Data brokers ought to be the last line of defense between personal

---

[178] *See, e.g.*, Millstone v. O'Hanlon Reports, Inc., 528 F.2d 829 (8th Cir. 1976); *see also* King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303 (E.D. Pa. 2012).

[179] *See supra* Part II.A–B.

information and a scammer. And yet, there is a clear narrative from the past fifteen years that voluntary efforts have not succeeded in controlling all data brokers or preventing bad actors. While some, like Acxiom, have changed their policies with regard to consumer access and correction of data,[180] most have not followed suit, if only for lack of the resources that Acxiom—a major multinational corporation—was able to put into building such an online portal.

In comparison, the public has fewer tools at its disposal. There are educational campaigns, but unless these achieve 100 percent effectiveness, scammers will invariably find and defraud those unaware of the scam. Another tool is the criminal prosecution of scammers, but for every scammer convicted, there are dozens more dead set on making a buck. This is the whack-a-mole problem, which persists despite threats of sentence enhancements and lengthy jail terms directed at would-be criminals.

Instead, policy makers should enact proactive measures that increase data brokers' responsibility to vet list buyers and shield sensitive consumer data. The FCRA provides a template for oversight that can be complemented by vicarious liability, meaningful opt-out options, and enhanced consumer education. This approach offers real protection for consumers without degrading the services data brokers provide.

A. Extend the Vetting Procedures of the FCRA

Congress should extend the FCRA concept of "legitimate business need" and "permissible purposes" to data

[180] *See* Singer, *supra* note 161.

broker lists.[181] The FTC should be tasked with reviewing illegitimate uses of lists and enforcing compliance. This section argues for this reform and describes how it might work.

1. Origins of the Data Broker Loophole

To this outside observer, it is clear that the FCRA created the data broker industry. In May 1969, Senator William Proxmire opened the five-day hearings with a premonition: "In the past, much of this information was hand-filed in local bureaus. However, the trend toward computers opens the way toward a gigantic national data bank which could include extremely personal information on every American citizen."[182] But Proxmire and his fellow Senators were short-sighted even as they foresaw computerized dossiers on every American. They focused on the problem of the day—inaccurate credit reports that could present financial hardships for those unable to access lines of credit. In tailoring their legislation to target the credit industry, Congress ensured the passage of the legislation. They also solved a controversy that consumers would be able to understand and would benefit immediately from the results. The credit issue was new enough, malicious enough, and time-consuming enough that other uses of personal information were left for a later day.

But the FCRA also left a new class of information unprotected. Marketing and individual reference data did not particularly offend the public and was not discussed overtly in the Fair Credit Reporting hearings.[183] But the concerns are equivalent: computerized files that make available extremely

---

[181] See discussion of the FCRA, *supra* Part III.D.I.
[182] *Fair Credit Reporting Hearing*, *supra* note 118, at 1–2.
[183] *See generally id.*

personal information on every American citizen. The line between the two classes of data is razor thin, as demonstrated by the FTC's recent Spokeo settlement where the FTC parsed out FCRA-covered practices of a data broker not overtly covered by the FCRA.[184] Furthermore, consumers have genuine concerns over their non-covered information. Aside from reputational harms, identity theft and stalking threats, and abusive marketing tactics, data broker lists may be used in scams that target vulnerable victims. The thinking behind the FCRA of promoting legitimate, transparent uses of credit reports should similarly apply to data broker lists.

2. Defining "Legitimacy"

An important FCRA provision restricts the sale of consumer reports to specified purposes, including legitimate business purposes.[185] In 1969, the Senate Committee noted that a television reporter was able to gain access to ten credit files by simply calling random credit bureaus under false pretenses.[186] This 'scandal' looks similar to the ChoicePoint release[187] and the recent hacking of major brokers as discussed above.[188] The same solution of limits on who can access the files could cut down on the fraudulent uses of the information. In particular, legislation should adopt the "legitimate business need" requirement,[189] which puts the onus on the data broker to determine if the information it sells will be used for a legitimate purpose. Under an FCRA regime, the FTC would be responsible for reviewing industry practices and would be able

---

[184] *See* Roth, *supra* note 117.
[185] *See* discussion of the FCRA, *supra* Part III.D.I.
[186] *See Fair Credit Reporting Hearing*, *supra* note 118, at 374.
[187] *See supra* note 68–70 and accompanying text.
[188] *See supra* Part III.
[189] *See* 15 U.S.C. § 1681b(a)(3) (2013).

to enforce fines and other sanctions for failure to adhere to the rules.

Just as the FCRA limits legitimate uses for certain purposes that primarily involve credit, insurance, and employment transactions, a data broker law would specify legitimate purposes for which a list might be conveyed from a data broker to another entity. Such legitimate purposes could include marketing campaigns involving direct solicitation. The data broker should be responsible to show that it knows the list user is engaged in a legitimate use. To do so, data brokers should review the marketing campaign and verify that the company actually has the capacity to sell the item it is marketing or has a contract to engage in telemarketing on behalf of another company. This review should not involve anonymous electronic vetting. That system, repudiated by the Second Circuit Court of Appeals, involves a list buyer selecting a permissible use for the list from a drop down menu without a more detailed review of that use.[190] Instead, the data broker should ask detailed questions about use and collect relevant documentation to verify legitimacy.

3. Penalizing Improper Vetting

Congress—or later, the FTC in rulemaking—should specifically identify suspect lists that merit added scrutiny. For instance, lists sold to marketers should not include protected phone numbers of individuals, such as telephone numbers listed on the national Do Not Call List.[191] If a data broker sells

---

[190] A user might be asked to select a statement saying the list will be used for marketing purposes only. *See* Gordon v. Softech Int'l, Inc., 726 F.3d 42, 57 (2d Cir. 2013); *see also* discussion of the DPPA, *supra* note 132.
[191] 15 U.S.C. § 6101 *et. seq*. (2013).

such a telephone number, the sale should be presumptively illegitimate without a specific showing of purpose.

Data brokers should face strong incentives to protect lists with sensitive information, such as a list consisting entirely of elderly individuals. State legislatures or Congress should consider enhancing penalties against data brokers when these types of lists are sold to an entity that was not fully vetted and then misused the information. Some privacy advocates have even argued that data brokers should be restricted from developing and selling lists on vulnerable adults of all types.[192] In testimony before the Senate Committee on Commerce, Science and Transportation, Pam Dixon described one list sold by a broker of "seniors who are currently suffering from dementia."[193] "A list of caregivers would not have the same potential for deleterious consequences," Dixon stated.[194] This argument is compelling because it singles out as prohibited the sale of lists of recognizably vulnerable individuals. That said, brokers will no doubt argue that marketers should have access to dementia patients to sell their cures. While this debate continues, data brokers should, at the very least, face stronger incentives to carefully vet users of these sensitive lists.

The FTC and state enforcement agencies might look more favorably on data brokers who place technical and contractual restrictions on list access. For instance, data brokers might develop a portal through which marketers could access names and contact individuals without ever seeing detailed information on the individual. The system would be designed to assist marketers in legitimate marketing

---

[192] *See, e.g.*, Dixon, *supra* note 62.
[193] *Id.*
[194] *Id.*

campaigns. As an example, a marketer would scroll through a list of truncated names and identifying information, click on the desired individual, and begin a phone call. Data brokers might also choose to rent rather than sell their lists, and contractually obligate the recipient to return the list at the conclusion of their marketing campaign. While these restrictions might be more costly to the data brokers, enforcement agencies could develop an incentive structure whereby a broker would face reduced liability in cases where these protective steps were taken, but the end user nonetheless misused the list.

4. Vicarious Liability for Misuse

Data brokers who fail to properly vet the legitimate business need of their clients ought to face liability for misuse of the lists. Data brokers should primarily face similar civil penalties to those of FCRA covered entities.[195] They should also be subject to criminal vicarious liability as exemplified in the outcome of the *Remsburg* decision, which found a broker vicariously liable for actions of a stalker using the broker's data.[196] This theory that brokers should be responsible for the uses of their databases has not been applied widely beyond New Hampshire but should apply especially when the data broker does not complete a full vetting process. Legislators could specifically implement vicarious liability legislation, or prosecutors could more aggressively identify and prosecute willful blindness, where a data broker could foresee misuse but does not take action to stop it.

---

[195] *See* 15 U.S.C. § 1681q (2013).
[196] *See* Remsburg v. Docusearch, Inc., 149 N.H. 148 (2003).

For enforcers, determining the source of a list may prove difficult. Right now, there are no requirements that brokers keep lists indicating the source of the information they resell or records of who obtained their information. Regulations should require brokers to maintain this information, in order to provide documentation relevant to future vicarious liability inquiries.

Does criminal vicarious liability go too far? Views no doubt will differ. For example, some might point to the case where the data broker genuinely made a mistake in the vetting process, but could nonetheless be held responsible for harm. The data broker might also not be fully responsible: for instance, a scammer might obtain a lead list from the data broker but supplement the list with more detailed facts that helped the scammer commit the crime. In some instances, the data broker might argue rightfully that the data broker itself was the true victim, because the scammer was able to outsmart the vetting process. And yet, on the other side of the equation are consumers who never expressly permitted the use of their personal information and who might be targeted. Data brokers should be liable for misuse, because the incentive will ensure they improve their vetting processes. As a result, improved vetting would deter scammers and, in the long run, ultimately reduce data broker liability. The data broker industry might argue successfully for a statutory cap on their overall vicarious liability. If negotiated carefully, such a cap could provide the desired incentive structure to vet list users without unduly burdening brokers.

5. Analysis of Likelihood of Implementation

Arguments against these restrictions focus on the potential sweeping nature of these reforms. FCRA type restrictions would bring changes to the industry and create new

regulatory burdens. They could jeopardize white pages directory services if not specifically exempted and could lead to new potential liability for non-data brokers if not carefully tailored.

Why not merely make data brokers illegal? Heavy-handed restrictions of this sort would put an end to the industry, but that is not in the interests of consumers or the data economy. First of all, some companies such as Acxiom have demonstrated a willingness to be more transparent, and they should not be penalized because of the practices of others in the industry.[197] And second, companies should have a chance to gain access to information about consumers in order to determine who should receive marketing material. In turn, consumers should expect transparent practices that are designed to protect that information from misuse. A narrowly-tailored set of laws that restrict companies that accumulate and resell data on a scale akin to that of large consumer reporting agencies would fill a gap that leaves much personal information vulnerable to misuse.

Unfortunately, Congress has shown such little interest in enacting any legislation—from gun control to immigration to food stamps—that the chances of data broker legislation actually passing are slim.[198] With the Edward Snowden leaks taking privacy debates in a different direction from commercial accumulation and use of data, the chances of reform today are

---

[197] *See* Singer, *supra* note 161.

[198] *See* Manu Raju, *The (Really) Do-Nothing Congress*, POLITICO (Nov. 11, 2013), http://www.politico.com/story/2013/11/the-do-nothing-congress-100274.html.

even lower.[199] Where data broker regulation was once part of Senator Patrick Leahy's privacy legislation, recent iterations have dropped all mention of not only data brokers but also data privacy, focusing almost exclusively on data security.[200] In the Senate, Senator Markey's legislation has a mere three cosponsors[201] and has just a three percent chance of enactment, according to the website GovTrack.[202] Other proposals, including potential regulatory actions that would increase scrutiny of data brokers doing business with the federal government is also unlikely given the widespread use of these brokers in the national security and law enforcement fields.[203]

B. Increase Consumer Control over Data Sharing

Even in a regime with strengthened vetting, consumer information is out there, and many consumers do not realize they are responsible. Consumers who fill out surveys or participate in store marketing programs lose control over their personal information, often without meaning to do so.[204] The result is that their personal information floats around from

---

[199] *See, e.g.*, Tom Ashbrook, *Tech Companies and American Privacy*, WBUR (Jan. 22, 2014), http://onpoint.wbur.org/2014/01/22/nsa-personal-privacy-constitutional-amendment.

[200] *Compare* S. 1490, *supra* note 172, *with* Personal Data Privacy and Security Act, S. 1897, 113th Cong. (2014) *and* Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015).

[201] *See* Data Broker Accountability and Transparency Act of 2015, S.668, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/668/cosponsors (last visited May 2015).

[202] *See S. 668: Data Broker Accountability and Transparency Act of 2015*, GOVTRACK.US, https://www.govtrack.us/congress/bills/114/s668 (last visited May 2015).

[203] *See* S. REP. NO. 111–110, *supra* note 174, at 25–29.

[204] *See* Trebilcock, *supra* note 54.

broker to broker, and some of it may one day be used fraudulently.

Senator Markey and former Senator Rockefeller want to see data brokers provide consumers a means to correct and access their data, and whether that legislation will pass one day is anyone's guess.[205] But that sort of system is not going to help consumers. Data brokers are not consumer-facing entities, and consumers simply do not know which ones to target when they have questions about their files.[206] The most vulnerable consumers will always be the ones who do not request their files or maintain control over their profiles. These are the consumers that the law should aim to protect.

A similar, but more powerful solution could create a national opt-out system akin to the successful FTC Do Not Call list[207]—a sort of Do Not Sell list that would prevent selling of certain personally identifiable information. Right now, many data brokers offer opt-outs, but these systems are often difficult to find, and data brokers are under no obligation to report to a consumer if their personal information is re-reported to the broker and reappears in the database.[208] A comprehensive Do Not Sell list solution would look different. A consumer would voluntarily register their name and zip code with a central database and select from a list of identifiers they would not want sold. For instance, Joe Smith would register that his zip code is 02454-3107 and select that he does not want his telephone number, date of birth, or race sold to a third party.

---

[205] See DATA Act, *supra* note 166 (introducing a bill, by Sen. Rockefeller and Sen. Markey, to require data brokers to establish certain procedures).
[206] *See supra* note 57.
[207] 15 U.S.C. § 6101 *et. seq*. (2013).
[208] *See, e.g.*, INTELIUS PRIVACY POLICY, INTELIUS, http://www.intelius.com/privacy.php (last visited Apr. 2014).

Data brokers would then be required to suppress that data from being resold. Sometimes, preventing a consumer's information from reappearing requires more data disclosure to the broker than mitigation, but under this system, the individual simply chooses the types of data to suppress without disclosing the data itself. This idea has not been endorsed by the industry and would require legislation to grant FTC authority to make these changes, similar to—and with many of the same limitations of—the legislation authorizing the Do Not Call list.[209]

C. Final Thoughts on Consumer Education

While education campaigns will never entirely prevent fraud, these campaigns should be more comprehensive. Consumer education should be directed toward controlling the information a consumer gives out in the first place, not just what to do when they receive a fraudulent phone call at three in the morning. Consumers should learn that they should treat their address, telephone, birth date, and other personal information just like their social security number. Consumers should learn about why a company or entity might ask for the data and learn to inquire as to how that information might be used. This type of change in thinking about personal information would not be favorable to the industry that has built a business around collection and resale of personal information, but it would better prepare consumers who more often than not have not heard about the grandparent scam or data brokers or Acxiom or the FCRA.

---

[209] 15 U.S.C. § 6101 *et. seq*. (2013).

V. CONCLUSION

Far too many older people do not realize that giving out personal information could land them on a list of people vulnerable to fraud.[210] With increased incidents of the grandparent scam, the dangers of widespread access to personal information are becoming more acute. The data broker industry responsible for spreading personal information around has not taken sufficient action to protect its data from falling into the wrong hands. Congress should extend the Fair Credit Reporting Act to the data broker industry, mandating that data brokers vet recipients of their lists to ensure data is used only for legitimate business purposes. In addition, consumers should be empowered to recognize the link between data disclosure and scams and to opt-out of data sharing. Stopping the grandparent scam will take more than consumer education and prosecuting offenders. One promising option is increased scrutiny of the lists that scammers use to target vulnerable consumers.

---

[210] *See* Nathalie Martin, *Consumer Scams and the Elderly: Preserving Independence Through Shifting Default Rules*, 17 ELDER L.J. 1, 27 (2009).