No. 13-1339

In The Supreme Court of the United States

SPOKEO, INC.,

Petitioner,

v.

THOMAS ROBINS, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

AMICUS CURIAE BRIEF OF CENTER FOR DIGITAL DEMOCRACY IN SUPPORT OF RESPONDENT

Of counsel:
ERIC G. NULL
1375 Kenyon St. NW
Apt. 515
Washington, DC 20010

ANGELA J. CAMPBELL
Counsel of Record
ANDREW JAY SCHWARTZMAN
INSTITUTE FOR
PUBLIC REPRESENTATION
600 New Jersey Ave. NW
Suite 312
Washington, DC 20001
(202) 662-9535
campbeaj@law.georgetown.edu

Counsel for Center for Digital Democracy

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

OTHER AUTHORITIES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

AMICUS CURIAE BRIEF OF CENTER FOR DIGITAL DEMOCRACY

INTEREST OF *AMICUS CURIAE*[1]

With the consent of all parties, *amicus curiae* Center for Digital Democracy ("CDD") submits this brief in support of Respondent, Thomas Robins. CDD agrees with the Ninth Circuit and the arguments put forth by Respondent that Robins has Article III standing to sue Spokeo under the Fair Credit Reporting Act ("FCRA") for publishing inaccurate personal information about himself. The purpose of CDD's *amicus curiae* brief is to explain the context in which this case arises: the pervasive collection, sale, and use of vast amounts of personal data that, if inaccurate, causes real harm to individuals.

CDD, a not-for-profit 501(c)(3) organization, is one of the leading consumer protection and privacy organizations in the United States. Since its founding in 2001 (and prior to that through its predecessor organization, the Center for Media Education), CDD has been at the forefront of research, public education, and advocacy protecting consumers in the digital age. CDD advocates before Congress and administrative

[1] No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the *Amicus Curiae*, its members, or its counsel made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief and such consents have been lodged with the Court.

agencies for policies and rules to ensure fair treatment of consumers by the financial, retail, health, advertising, and other industries. For instance, CDD has advised the Federal Trade Commission regarding the prevalence and harms caused by mobile device tracking. CDD also informs consumers, regulators, and the news media about contemporary digital information collection and use practices, such as data brokers' use of algorithms in "programmatic" advertising, via its website, blog, and public reports at http://www.democraticmedia.org.

SUMMARY OF ARGUMENT

This brief provides the Court with additional background information regarding harms experienced by individuals caused by data brokers such as Spokeo. Data brokers collect vast amounts of data about individuals browsing the Internet or using their smartphones, combine these data with data from other sources (which can be inaccurate or unreliable), create profiles of individuals, categorize individuals into groups such as "Hard Times" and "X-tra Needy" for marketing purposes, and sell these data to third parties that use the data to make important and sensitive decisions about employment, credit, and other aspects of people's lives. Because data brokers collect so much information about so many different people from so many sources, inaccuracies are inevitable.

When inaccurate data are used to make decisions about individuals, they experience real harm. For example, if a potential employer decides whom to interview based on inaccurate data, well-qualified individuals may be excluded from consideration. Similarly, given the sophisticated targeting methods employed in digital marketing, offers targeted based on inaccurate data will mean that individuals may be inappropriately associated with ads about arrest records or may be targeted with payday loans when they could otherwise obtain better loan terms.

ARGUMENT

I. DATA BROKERS HARM INDIVIDUALS WHEN THEY COLLECT AND SELL INACCURATE DATA.

Data brokers ("brokers"), including Spokeo, are "companies that collect consumers' personal information and resell or share that information with others." *Data Brokers: A Call for Transparency and Accountability*, Federal Trade Commission at i (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (hereinafter "FTC Report"). Brokers have become persuasive and powerful entities because of technological changes that have made tracking individuals and collecting, analyzing, and storing data inexpensive and easy. Additionally, data processing techniques have evolved such that data collected for one

purpose can now be used for any number of purposes for which it was not originally collected. *See* FTC Report, at vii; Steve Kroft, *The Data Brokers: Selling Your Personal Information*, "60 Minutes," CBS News (Mar. 9, 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information. They have grown so large that the top 100 websites "are monitored by more than 1,300 firms," which includes data brokers. Simon Board & Jay Lu, *Competitive Information Disclosure in Search Markets*, at 2 n.1 (Aug. 15, 2015), http://www.econ.ucla.edu/sboard/papers/infosearch.pdf. With such a broad reach online, it is nearly impossible for individuals to avoid being tracked.

While companies other than brokers collect data about individuals both online and offline (such as Google, Facebook, and other advertising companies), this brief focuses on data brokers like Spokeo. This brief will explain what information brokers collect, how they use and sell the information, and how individuals can experience harm as a result of disseminating inaccurate information.[2]

[2] This brief uses "data" and "information" interchangeably unless otherwise noted.

A. Brokers collect an unprecedented amount of data, which can be inaccurate.

Recently, the Federal Trade Commission and the Senate Commerce Committee studied brokers in part because they have become ubiquitous online yet the public knows very little about them. FTC Report, at 7. Concerns also grew that they were acting in secret and taking advantage of consumers. *A Review of the Data Broker Industry*, Senate Commerce Committee at i (Dec. 18, 2013), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 (hereinafter "Senate Report").

Three of the primary findings of these reports, which are explained below, were (1) brokers collect an unprecedented amount of information about individuals, (2) brokers collect data from a variety of sources including other data brokers, but the data's accuracy is not guaranteed, and (3) individuals often lack meaningful controls over those data.

1. Brokers fill massive databases with sensitive and personal data about individuals.

Brokers continually collect data about almost every individual and almost everything those individuals do online and offline, creating massive data sets. BlueKai, a broker now owned by Oracle Corporation, "compiles around 1 billion profiles of potential customers around the world, each with an average of

50 attributes." *Getting to Know You*, Economist (Sept. 13, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party. The broker Acxiom "has 'multi-sourced insight into approximately 700 million consumers worldwide,' and Datalogix [another broker] asserts its data 'includes almost every U.S. household.'" Senate Report, at 12 (internal citations omitted). Further, the broker and credit scoring company Equifax "maintains approximately 75,000 individual data elements for its use in creating marketing products." *Id*. at 14.

The data collected by brokers are extensive, personal, and sensitive. They include, for example,

- identifying data (name, social security number, driver's license number, birth dates for the individual and all individuals in the household),
- device browser history (types, methods, and costs of purchases, online activities, location, content viewed, items placed in online shopping carts from a personal computer or mobile device),
- court data (criminal convictions, bankruptcies, judgments, liens),
- health data (disability, weight loss & supplements, geriatric supplies),
- loyalty card data (from retail stores and mobile applications), and

- financial data (household income, credit worthiness, ability to afford products, actual purchase data).

See FTC Report, App'x B; Senate Report, App'x II & III, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0cecef67-8e18-4bcb-b867-2a8e13d552f7; *see also IXI Digital Targeting Options*, IXI Digital, https://www.ixicorp.com/ixi-digital/ixi-digital-targeting-options (providing products for targeting consumers based on, among other things, wealth, mortgage propensity, and ability to pay). These data come from both online and offline sources, which can be merged, creating comprehensive personal profiles. FTC Report, at 47.

"Raw" data elements, such as name, address, telephone number, and purchase history, are called "actual" elements. A broker may then infer certain characteristics based on those "actual" data elements, which are called "derived" elements. Brokers use derived elements to predict personal interests or may attempt to categorize individuals based on sensitive personal characteristics. Harlan Yu, *Data Brokers Target the "Urban Scramble,"* EqualFuture (May 28, 2014), https://www.equalfuture.us/2014/05/28/data-brokers-target-the-urban-scramble.

Brokers obtain seemingly endless data points because they collect data from a variety of sources as companies attempt to stay current with individuals' interests and modes of communication. *Merkle Data Management Cloud*, Merkle, http://www.merkleinc.

com/what-we-do/marketing-technology/merkle-data-management-cloud (Merkle "meets the evolving needs of brands by enabling the most relevant customer experiences that lead to deeper customer relationships.").

2. Brokers Collect and Pool Data from a Variety of Sources, Including Other Data Brokers, Which Likely Contains Inaccurate Data.

Brokers collect and pool data from as many sources as possible. Most commonly, brokers share and sell with each other the information they compile such as data from telephone companies about consumers receiving new landline accounts, data from automobile dealers about sales, service, warranty, and aftermarket repairs, and data from offline sources such as marketing surveys, warranty registrations, and contests. FTC Report, at 13-14; Senate Report, at 16. Brokers also purchase retail-transaction-specific data from retailers, which includes the type, date, and dollar amount of each purchase and the type of payment used. FTC Report, at 13; Senate Report, at 16. "Registration" websites, such as news and travel sites, sell data they receive through account registrations. FTC Report, at 13. Additionally, some brokers obtain data directly from financial institutions. Senate Report, at 16.

Brokers collect data from governmental sources as well. The Federal government houses data from, for instance, the Census and the Death Master File,

which includes the Social Security Numbers of deceased individuals. Federal courts provide information on bankruptcies. State and local governments provide data including property records, taxes, professional or recreational licenses, voter registrations, and court records. FTC Report, at 11-12.

A significant amount of data comes from online tracking of individuals and mining publicly available online sources. Tracking and data analysis technologies pervade the Internet and mobile devices. These technologies are, in most cases, surreptitiously installed on the individual's device, such as cookies, Flash cookies, and web beacons. *Tracking the Trackers: What Are Cookies?*, Guardian (Apr. 23, 2012), http://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro. Once installed, they collect data about purchases made, websites visited, content viewed, time spent on those websites, location, browser history, browsing habits, and other data unbeknownst to consumers (so-called "passive" collection). *See Policy on Passive Electronic Data Collection*, Oregon Dept. of Transportation (Mar. 12, 2015), http://www.oregon.gov/ODOT/TD/TP/Plans/ADM%2008%2001.pdf ("Passive [data collection occurs when] the customer has little or no awareness of the data being collected and requires no explicit actions on the customer's part."). A report by the *Wall Street Journal* in 2010 found that the top 50 websites installed an average of 64 trackers on their visitors' browsers. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, Wall St. J. (July 30, 2010), http://www.wsj.com/

articles/SB10001424052748703940904575395073512989404.

Where tracking technologies are insufficient, such as on mobile devices, brokers turn to other methods to profile users. Some invoke an individual's unique mobile device identifier, which can also track and profile that individual across multiple devices. Allison Schiff, *A Marketer's Guide to Cross-Device Identity*, AdExchanger (Apr. 9, 2015), http://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity. These techniques, however, have not been standardized, meaning data collected in this way is often inaccurate. Mobile location data is particularly inaccurate. *See, e.g.*, Steven Jacobs, *Report: More Than Half of Mobile Location Data Is Inaccurate*, StreetFight (May 14, 2015), http://streetfightmag.com/2015/05/14/report-more-than-half-of-mobile-location-data-is-inaccurate.

Through online data mining, brokers acquire a lot of personal data through automated processes. Brokers typically mine data from publicly available online sources with "web crawlers, which are programs that capture content across the Internet and transmit it back to the data broker[]." FTC Report, at 17. For example, they may mine social media sites such as Facebook and LinkedIn, where individuals upload a great deal of information about what they do, what they like, what their political views are, as well as photos and videos to share with their friends, family, or colleagues. *See, e.g.*, *Data Provider PeekYou Leverages SpatialKey to Maximize Sales and Help*

Clients Better Understand their Customers' Social Media Activity, SpatialKey, https://www.spatialkey.com/assets/pdf/Market_Intelligence/SpatialKey__PeekYou_Case_Study.pdf ("PeekYou [offers a data-mining service that] analyzes activity on social networks and other public websites and then builds detailed profiles of the individuals behind that activity. PeekYou's profiles include the ages, locations, incomes, and interests of more than 250 million people."). Brokers also use data mining techniques on sites that collect information through registration sites and blogs. FTC Report, at 13. This kind of collection is known as "active" collection because the individual actively provides the information. *Policy on Passive Electronic Data Collection*, *supra* at 2. Typically, however, the individual provides the information for one purpose, such as ordering a book or sharing pictures of their dog with family, and are not aware that this information is mined by brokers for other purposes. *See* Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L.Rev. 1880, 1902 (2013) ("data can potentially be used in harmful ways that people might not be able to anticipate or understand.").

Brokers increasingly collect data, such as purchase and warranty data, from offline sources. FTC Report, at 1-2, 27. Offline data are tremendously valuable because offline activities can provide further insight into individuals' purchasing habits or even voting record. Lois Beckett, *Everything We Know About What Data Brokers Know About You*,

ProPublica (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. Brokers continually merge that offline data with online data, the combination of which the broker sells. FTC Report, at 27; *see also Neustar CRM Onboarding*, Neustar, https://www.neustar.biz/resources/product-literature/crm-onboarding-solution-sheet.

Brokers amass enormous data sets from hundreds of sources, but those data are not guaranteed to be accurate and in fact can be very inaccurate. Experian, a broker, released a study recently finding a "high degree of inaccurate information" contained in broker databases, with U.S. organizations claiming that thirty-two percent of their data is inaccurate. *New Experian Data Quality Research Shows Inaccurate Data Preventing Desired Customer Insight*, PR NewsWire (Jan. 28, 2015), http://www.prnewswire.com/news-releases/new-experian-data-quality-research-shows-inaccurate-data-preventing-desired-customer-insight-300025513.html; *see also* Erin Haselkorn, *The Biggest Data Quality Challenges*, Experian (June 10, 2014), http://www.experian.com/blogs/marketing-forward/2014/06/10/the-biggest-data-quality-challenges. Even government data can be inaccurate, which in one case led to likely incorrect Congressional testimony because data was not transferred to the right people. Katherine Barrett & Richard Greene, *The Causes, Costs and Consequences of Bad Government Data*, Governing (June 24, 2015), http://www.governing.com/topics/mgmt/gov-bad-data.html.

Studies have also shown that profiles often misrepresent the individual. A 2014 study of eight online profiles found that "[a]ll profiles had errors to varying degrees." One participant's profile overstated his situation by claiming that, similar to Robins, "the participant was affluent with 350000+ income, had top 1% credit and owned [an] American Express card." Ashwini Rao, *et al*., *What Do They Know About Me?*, 2014 Harvard ASE Conference, http://www.ase360.org/bitstream/handle/123456789/191/P39.pdf, at 7. *See also* Maureen Mahoney, *Errors and Gotchas*, Consumers Union (Apr. 9, 2014), http://consumersunion.org/wp-content/uploads/2014/04/Errors-and-Gotchas-report.pdf (describing credit reporting errors that are "too common"). The news media has also exposed inaccurate data collected by brokers, including Spokeo. Lindsay Riddell, *Spokeo: What Do They Know About You?*, S.F. Bus. Times (Jan. 13, 2011), http://www.bizjournals.com/sanfrancisco/blog/2011/01/remove-yourself-from-spokeo.html ("Spokeo says I am single. (News to my husband). Spokeo says I live with my parents. (Not for a very long time). Spokeo says I am a male. (Untrue for multiple provable reasons). Spokeo says I've lived in my house for 1 year. (I've lived there for three)."). These data may never be corrected because brokers may never have to update their data after initial collection. FTC Report, at 18.

For purposes of showing that data can often be inaccurate, counsel for CDD obtained his profile from Acxiom at "Aboutthedata.com." The profile for Eric G. Null misrepresented, among other things, that he has

only a high school education, even though he has graduated law school, and owns a home with a market value of $500,000-$749,999, when he in fact rents an apartment.

"With so much information coming from so many sources, it is inevitable that errors arise in" data collection. Gary Anthes, *Data Brokers Are Watching You*, 58 Comms. of the ACM 28 (Jan. 2015), http://cacm.acm.org/magazines/2015/1/181629-data-brokers-are-watching-you/fulltext. Unfortunately, individuals are unlikely to have the ability to correct inaccurate data about them.

3. Individuals generally cannot correct errors in data held by brokers.

As established above, brokers collect a significant amount of inaccurate data, which is used to make sensitive decisions about them. Rarely, however, can an individual access their complete profile or correct errors.

Some brokers have attempted to be transparent about the data they collect, but those attempts have been inadequate. For example, Acxiom created the site "Aboutthedata.com" for individuals to view data the company has collected about them. This site, however, provides consumers access to only "raw" data (e.g., name, address, income), not segments or derived data, Senate Report, at 34, which are often the most problematic elements. *See* FTC Report, at 42 ("data brokers typically provide access to raw data

and not to their proprietary information that they derive through algorithms.").

Other entities have not attempted to be transparent. Experian and Equifax provide no right to view or correct data collected by them because they claim their data is "anonymized," meaning they remove identifying information such as the individual's name. Senate Report, at 33-34. However, anonymizing data has failed to protect individuals against being identified. Researchers have shown that "third part[ies] could match . . . browsing histories [likely stored in cookies] against identified datasets to re-identify them." Jonathan Mayer & John Mitchell, *Third-Party Web Tracking: Policy and Technology*, 2012 IEEE Symposium on Security and Privacy 413, 416, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427.

Data about individuals are often collected for one purpose and sold for another, which is difficult for an individual to understand and predict. For instance, Whitepages.com says it collects data from third-party data suppliers, which may include data from "contests, sweepstakes, subscriptions or other similar offers." *Where Do You Get Your Information From*, Whitepages (Oct. 22, 2014), https://support.whitepages.com/hc/en-us/articles/203263894-Where-do-you-get-your-information-from. The individuals that disclose their data in those contexts (offline and for a specific purpose, namely, entering a contest) likely do not understand their data will be sold to Whitepages.com and other third parties for anyone online to find.

Solove, *supra*, at 1902 (stating there may be "[n]ew ideas for combining data, new discoveries in data aggregation and analysis, and new techniques and technologies of data analysis . . . [that may] potentially be used in harmful ways that people might not be able to anticipate or understand.").

Without a meaningful ability to correct data, individuals cannot protect themselves or ensure their data are accurate.

B. Brokers use compiled data to profile individuals algorithmically and sell those profiles for a variety of purposes.

Brokers put their data to a variety of uses, but first have to compile the data they have collected into very detailed profiles. The underlying data in these profiles are then passed through algorithms that ultimately determine into what "segments" the individual will be placed or how they will be classified, such as if the individual needs a loan or purchases fast food. Then, brokers can sell these profiles or lists of individuals for marketing, risk mitigation, and people search purposes.

1. Brokers compile data about individuals into detailed profiles and place those individuals into "segments" based on those profiles.

Brokers compile data about specific individuals into profiles. The aggregated or consolidated data points create a rich picture of who the individual is.

Brokers curate their data through derived data elements (discussed above) and by assigning individuals to certain "segments" based on the actual and derived data elements in their profile. FTC Report, at 19. Many segments are designed to target financially vulnerable populations: X-tra Needy; Zero Mobility; Hard Times; Enduring Hardships; Small Town Shallow Pockets; Burdened by Debt: Singles; Rural and Barely Making It; and Financially Challenged. Senate Report, at 24; FTC Report, at 21. Some segments focus on other characteristics: Downtown Dwellers; Plus-size Apparel; Bible Lifestyle; Latchkey Leasers; and others. FTC Report, at 20 n.52 & 21. Segments are often defined; for example, Experian defines "Hard Times" in part as "the bottom of the socioeconomic ladder, the poorest lifestyle segment in the nation." Senate Report, at 25.

Once brokers assign segments to individuals, they can create lists of individuals believed to have those traits or to exhibit those predicted behaviors. These lists are then sold to third parties. For instance, a bank may want to know whether any of its customers are on the "Financially Challenged" or "Hard Times" list before they make an online offer for a credit card at an attractive interest rate or target someone for a high-cost student loan for a private college. *Private For-Profit Colleges and Online Lead Generation: Private Universities Use Digital Marketing to Target Prospects, Including Veterans, via the Internet*, Center for Digital Democracy (May 2015),

https://www.democraticmedia.org/article/private-profit-colleges-and-online-lead-generation.

Brokers handle immense data sets, analysis of which is beyond the means of any human. Therefore, brokers rely extensively on "algorithms" that are processed via computers. Algorithms, which are essentially a series of automated steps applied to data, analyze data sets, identify patterns and relationships (correlations), generate categories for filtering information (segments), and otherwise help in analyzing vast amounts of data. *Big Data: Seizing Opportunities, Preserving Values*, White House at 46 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Algorithmically assigning segments based on inaccurate data can have serious consequences for individuals because third parties, such as employers and marketers, make sensitive decisions about individuals based on those segments

2. Brokers sell profiles, including segments, for numerous purposes.

Brokers sell their data for many purposes, including marketing, verification of an individual's identity,[3] and "people search." Brokers have devised several marketing-related products designed to target individuals or grow marketing campaigns. One

[3] This brief will not focus on sale of data for identity verification.

product is "data append," where a client seeks a more complete profile of its customers, which a broker can provide, for traditional or online marketing purposes. FTC Report, at 24, 26. Further, through a process called "onboarding," brokers can load offline data into a browser cookie "to enable advertisers to target consumers" with advertisements based on offline activity. FTC Report, at 27. Brokers can also provide analytics that attempt to predict individuals' likely behavior. Analytics can also be used to "score" (like a credit score) certain individuals based on "how likely they are to respond to particular marketing efforts" or whether an individual has a low purchase rate. FTC Report, at 31. These methods create highly individualized and targeted marketing campaigns.

Profiles are relevant to auctioning online advertisements. Advertisers buy the right to serve an advertisement to a specific individual in real-time through auctions. These decisions are often made based on the profile of and segments assigned to the individual. The entire auction process takes less than fifty milliseconds. *Real-Time Media Buying: Advertise Online in a Smarter and More Efficient Way*, Exact Drive, http://www.exactdrive.com/real-time-media-buying. The speed at which advertisers purchase the right to advertise gives consumers even less control over how companies use their data.

Brokers can also sell their profiles for use with "people search" products, which is a product Spokeo provides. "People search" companies collect substantial

personal information about individuals, such as social security number, marriage or divorce records, and employment history, from a variety of sources. Then, they release that information in compiled form online for anyone to see. FTC Report, at 34. People may visit these sites to find out information about their friends or relatives, or employers could use these databases to gain more information about applicants. Many "people search" services, including Spokeo, tell their users not to use their data for "purposes governed by the FCRA, including eligibility for employment, credit, insurance, housing, or similar purposes." FTC Report, at 35; *see also* Complaint at 5, *United States v. Spokeo, Inc*., No. CV12-05001-MMM-SH (C.D. Cal. June 7, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeocmpt.pdf. However, as discussed below, those uses occur nonetheless, and a simple disclaimer is insufficient to avoid causing significant harm.

C. Individuals experience real harm when decisions are made about them based on inaccurate information.

In addition to the uses above, data are used in employment and advertising contexts. Further, these data can be used to engage in discrimination based on protected classes such as race. Because many companies use data to make sensitive and personal decisions, data must be accurate or else these individuals will experience substantial harm.

1. Employers use profiles, algorithms, and online sources to make hiring decisions, which can be based on inaccurate information and can harm individuals.

Employers have increasingly relied on profiles, algorithms, and online sources in hiring. These services reduce costs in the hiring process and help employers gain insight into and information about applicants via automated screening. *E.g.*, Leigh Buchanan, *Unemployment Is Up. Why Is It So Hard to Find the Right Hires?*, Inc. (June 1, 2012), http://www.inc.com/leigh-buchanan/hiring-recruiting-unemployment-wharton-peter-cappelli.html. However, these efforts can have unintended consequences for individuals seeking employment. For example, "[v]eterans have complained that they were automatically disqualified for civilian jobs because [algorithms] . . . didn't recognize the skills they learned in the military." Elizabeth Dwoskin, *How Social Bias Creeps Into Web Technology*, Wall St. J. (Aug. 21, 2015), http://www.wsj.com/article_email/computers-are-showing-their-biases-and-tech-firms-are-concerned-1440102894-lMyQjAxMTI1NzI3NjMyNjY2Wj. Further, "Carnegie Mellon University researchers examining Google's ad-targeting system recently found that male Web users were six times more likely than female users to be shown ads for high-paying jobs." *Id*. These decisions, made by algorithms, have significant effects on an individual's ability to obtain a job and may result in long term unemployment.

Even if a human reviews data about an applicant, inaccurate data can still lead to adverse decisions that harm individuals. Employers rely on publicly available sources online and often obtain background checks and review credit reports. Alexander Reicher, *The Background of Our Being: Internet Background Checks in the Hiring Process*, 28 Berkeley Tech. L.J. 115, 118-20 (2013); Jeanne Sahadi, *Background Checks: What Employers Can Find Out About You*, CNN Money (Jan. 5, 2015), http://money.cnn.com/2015/01/05/pf/background-checks; Lea Shepard, *Seeking Solutions to Financial History Discrimination*, 46 Conn. L. Rev. 993, 1005 (Feb. 2014). Credit reports, in particular, are heavily relied upon. However,

> [j]ob applicants with adverse credit histories – those that reflect collection actions, bankruptcies, or high debt-to-income ratios – are at a competitive disadvantage. Employers are prone to make a multitude of negative assumptions about such individuals: they are more likely to be irresponsible, more likely to commit fraud or theft on the job, more susceptible to bribery and blackmail, or more likely to be distracted by financial worries or collection activity.

Shepard, *supra*, at 996. Thus, "a job applicant would be wise to scrutinize his report in advance of an employer's formal vetting process to ensure that no information in the report is incomplete or inaccurate." *Id.* at 995. If there are errors on an individual's credit report, employers are likely to find out and may make

negative inferences about the individual to his or her detriment. As discussed above, data stored in a broker's database is virtually inaccessible and individuals likely cannot access their profiles to correct any errors.

Algorithmic discrimination based on protected classes likely occurs in employment. "[A]lgorithms can obscure discrimination," can "sort[ ] resumes according to fuzzy, non-transparent criteria," and may make "correlations between protected-class characteristics like race or sex, and the traits that predict employee success." Alex Rosenblat *et al*., *Networked Employment Discrimination*, Data & Society Research Inst., http://www.datasociety.net/pubs/fow/EmploymentDiscrimination.pdf at 9. For example, discrimination can result by use of proxies – using data that is roughly correlated to race or gender. ZIP Codes can correlate to race, which means algorithms, or even humans, may discriminate based on race simply by removing certain ZIP Codes from their applicant pool. Katherine Noyes, *Will Big Data Help End Discrimination – or Make It Worse?*, Fortune (Jan. 15, 2015), http://fortune.com/2015/01/15/will-big-data-help-end-discrimination-or-make-it-worse. Xerox used to filter its applicants for commute time which "could put applicants from minority neighborhoods at a disadvantage in the hiring process." Dwoskin, *supra*. These and similar filtering decisions, which may seem innocuous, could effectively filter out certain races or genders. If the algorithm or employer relies on inaccurate data about race, gender, disability, or even

proxies such as ZIP Code, the repercussions for that individual can be significant.

Individuals experience harm when decisions about their employment are made based on inaccurate data. However, this is not the only context in which inaccurate data can be used to harm individuals.

2. Individuals experience harm by being targeted with ads based on race or similarly sensitive characteristics.

Brokers and the advertising industry are inextricably linked. As discussed above, brokers provide data to support targeted advertising and can help companies target consumers in countless ways. Many segments are specifically designed to target advertising to individuals based on traits and predicted behaviors. FTC Report, at 19. Targeting individuals based on inaccurate data, however, can significantly harm consumers.

Advertising suffers from discrimination in data collection and use. Latanya Sweeney, a Harvard University Professor and former FTC Technologist, released a study in 2012 concluding that, while using Google AdSense and InstantCheckmate.com, searches for names typically associated with African-Americans were more likely to display ads with "arrest" in the text than searches for names typically associated with White people. Latanya Sweeney,

Discrimination in Online Ad Delivery, Data Priv. Lab (Jan. 28, 2013), http://dataprivacylab.org/projects/onlineads/1071-1.pdf, at 34. This study stands for the proposition that algorithms can reflect biases and inaccurate stereotypes that pervade society, and thus perpetuate them. The most obvious harm resulting from this algorithmic misstep is giving the likely false impression (to employers, friends, or anyone who Google-searches the name) that the individual has been arrested, which can automatically remove that individual from consideration for many benefits.

Further, marketers harm consumers by targeting ads for less desirable products and services such as payday loans. Ed Mierzwinski & Jeff Chester, *Selling Consumers Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act*, 46 Suffolk L.Rev. 845, 849 (2013); Nathan Newman, Comments, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population*, FTC Workshop, Big Data: A Tool for Inclusion or Exclusion?, https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf. For instance, an individual with a relatively low-income, or who may live in a particular low-income ZIP Code, may receive targeted advertisements for payday loans when that individual could otherwise qualify for more favorable terms. This may have serious consequences for the consumer because payday loans have extremely high interest rates and often target minorities and low-income households. Raúl Arce-Contreras, *A Word*

of Caution on Payday Loans, Center for Am. Progress (Apr. 7, 2009), https://www.americanprogress.org/issues/regulation/news/2009/04/07/5850/a-word-of-caution-on-payday-loans.

Thus, individuals clearly experience substantial harm as a result of dissemination of inaccurate information about them.

CONCLUSION

Brokers and other companies constantly collect, use, and sell online and offline data about individuals that help third parties make millions of data-driven decisions in sensitive contexts such as employment, marketing, and finance. Any such decision based on inaccurate data is very likely to cause serious harm to that individual.

Respectfully submitted,

Of counsel:
ERIC G. NULL
1375 Kenyon St. NW
Apt. 515
Washington, DC 20010

ANGELA J. CAMPBELL
Counsel of Record
ANDREW JAY SCHWARTZMAN
INSTITUTE FOR
PUBLIC REPRESENTATION
600 New Jersey Ave. NW
Suite 312
Washington, DC 20001
(202) 662-9535
campbeaj@law.georgetown.edu

Counsel for Center for Digital Democracy