

No. 13-1339

In the Supreme Court of the United States

SPOKEO, INC.,

Petitioner,

v.

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

Respondent.

*On Writ of Certiorari to the United States
Court of Appeals for the Ninth Circuit*

**BRIEF OF AMICI CURIAE STATES OF MASSACHUSETTS,
CONNECTICUT, DELAWARE, THE DISTRICT OF COLUMBIA,
HAWAII, ILLINOIS, MAINE, MARYLAND, MINNESOTA,
MISSISSIPPI, NEW MEXICO, NEW YORK, OREGON, AND
WASHINGTON IN SUPPORT OF RESPONDENT**

MAURA HEALEY

Attorney General of Massachusetts

SARA CABLE*

FRANCESCA L. MICELI

Assistant Attorneys General

Office of the Attorney General

One Ashburton Place

Boston, MA 02108

(617) 727-2200

sara.cable@state.ma.us

**Counsel of Record for Amici Curiae*

(Additional Counsel on Inside Cover)

GEORGE JEPSEN
Attorney General
of Connecticut
55 Elm St.
Hartford, CT 06106

MATTHEW P. DENN
Attorney General
of Delaware
820 N French St., 6th Fl.
Wilmington, DE 19801

KARL A. RACINE
Attorney General
for the District of Columbia
441 4th St., NW
Washington, DC 20001

DOUGLAS S. CHIN
Attorney General
of Hawaii
425 Queen St.
Honolulu, HI 96813

LISA MADIGAN
Attorney General
of Illinois
100 W. Randolph St.
12th Floor
Chicago, IL 60601

JANET T. MILLS
Attorney General
of Maine
109 Sewall St.
Cross Office Building
6th Floor
Augusta, ME 04330

BRIAN E. FROSH
Attorney General
of Maryland
200 Saint Paul Pl.
Baltimore, MD 21202

LORI SWANSON
Attorney General
of Minnesota
102 State Capitol
75 Rev. Dr. Martin Luther
King Jr. Blvd.
St. Paul, MN 55155

JIM HOOD
Attorney General
of Mississippi
P. O. Box 220
Jackson, MS 30205

HECTOR H. BALDERAS
Attorney General
of New Mexico
P. O. Drawer 1508
Santa Fe, NM 87504

ERIC T. SCHNEIDERMAN
Attorney General
of New York
120 Broadway
25th Floor
New York, NY 10271

ELLEN F. ROSENBLUM
Attorney General
of Oregon
1162 Court St. N.E.
Salem, OR 97301

ROBERT W. FERGUSON
Attorney General
of Washington
1125 Washington St. SE
P.O. Box 40100
Olympia, WA 98504

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
INTERESTS OF <i>AMICI CURIAE</i>	1
SUMMARY OF ARGUMENT	2
ARGUMENT	4
I. CONSUMERS ARE ROUTINELY HARMED BY THE DISSEMINATION AND USE OF INACCURATE DATA PROFILES	4
A. Vast Amounts of Detailed, Personal Consumer Data Are Collected, Processed, and Sold By the Data Broker Industry	5
B. Businesses Frequently Rely on Data Profiles to Make Decisions With Important Consequences for Consumers	11
C. Error-Prone Consumer Data Profiles Lead to Negative Consequences that Consumers Are Unable to Identify	16
II. THE FCRA IS A CRITICAL TOOL TO PROTECT CONSUMERS FROM THE DISSEMINATION OF INACCURATE DATA PROFILES	19
A. The FCRA Is Intended to Protect Consumers Against the Dissemination of Inaccurate Data Profiles by Data Brokers	21
B. Harm to Reputation or Property Rights, Even Without Proof of Additional Injury, Has Been Long Understood to Create a Judicable Case	22

C. The Dissemination of Inaccurate Personal Data Causes a Substantial Risk of Injury Sufficient for Standing	26
D. Statutory Damages Cases and Private Class Actions Are Needed to Complement the Role of Attorneys General in Protecting Consumers	33
CONCLUSION	37

TABLE OF AUTHORITIES

CASES

<i>Bateman v. American Multi-Cinema,</i> 623 F.3d 708 (9th Cir. 2010)	34
<i>Beaudry v. Telecheck Services,</i> 579 F.3d 702 (6th Cir. 2009)	26
<i>Clapper v. Amnesty Int’l USA,</i> — U.S. —, 133 S. Ct. 1138 (2013)	26, 27, 28
<i>F.W. Woolworth Co. v. Contemporary Arts, Inc.,</i> 344 U.S. 228 (1952)	25
<i>Feltner v. Columbia Pictures Television, Inc.,</i> 523 U.S. 340 (1998)	25
<i>Figueroa v. Sharper Image Corp.,</i> 517 F. Supp. 2d 1292 (S.D. Fla. 2007)	36
<i>Harris v. Mexican Specialty Foods, Inc.,</i> 564 F.3d 1301 (11th Cir. 2009)	34
<i>Holman v. Experian Info. Solutions, Inc. et al,</i> C.A. No. 11-00180, Dkt. No. 279 (N.D. Cal. Dec. 29, 2014)	35
<i>In re Adobe Sys., Inc. Privacy Litig.,</i> 66 F. Supp. 3d (N.D. Cal. 2014)	27, 28, 30
<i>Krottner v. Starbucks Corp.,</i> 628 F.3d 1139 (9th Cir. 2010)	28
<i>Lujan v. Defenders of Wildlife,</i> 504 U.S. 555 (1992)	23

<i>Marzetti v. Williams</i> , 1 B. & Ad. 415, 109 Eng. Rep. 842 (K.B. 1830)	24
<i>Mass. v. Env'tl. Prot. Agency</i> , 549 U.S. 497 (2007)	33
<i>Meese v. Keene</i> , 481 U.S. 465 (1987)	24
<i>Murray v. GMAC Mortg. Corp.</i> , 434 F.3d 948 (7th Cir. 2006)	34, 36
<i>Remijas v. Neiman Marcus Group, LLC</i> , Dkt. No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015)	27, 28, 30
<i>Rude v. Westcott</i> , 130 U.S. 152 (1889)	24
<i>Steel Co. v. Citizens for a Better Env't</i> , 523 U.S. 83 (1998)	24
<i>Tyler v. Michaels Stores, Inc.</i> , 464 Mass. 492 (2013)	25
<i>Whittemore v. Cutter</i> , 29 F. Cas. 1120 (C.C.D. Mass. 1813)	25
<i>Wilson v. DirectBuy, Inc.</i> , No. 3:09-CV-590JCH, 2011 WL 2050537 (D. Conn. May 16, 2011)	36
<i>Zivotofsky v. Kerry</i> , ___ U.S. ___, 135 S. Ct. 2076 (2015)	26

STATUTES AND REGULATIONS

15 U.S.C. §§ 1681 <i>et seq.</i>	<i>passim</i>
15 U.S.C. § 1681(a)(2)	19
15 U.S.C. § 1681(a)(3)	21
15 U.S.C. § 1681(a)(4)	20
15 U.S.C. § 1681(b)	21
15 U.S.C. § 1681a(b)	21
15 U.S.C. § 1681a(d)	21, 26
15 U.S.C. § 1681a(d)(1)	21, 22, 26
15 U.S.C. § 1681a(f)	21, 26
15 U.S.C. § 1681b	26
15 U.S.C. § 1681b(a)	22, 26
15 U.S.C. § 1681e(b)	<i>passim</i>
15 U.S.C. § 1681n	22
15 U.S.C. § 1681n(a)	26
15 U.S.C. § 1681n(a)(1)(A)	34
15 U.S.C. § 1681n(a)(2)	34
15 U.S.C. § 1681o	22
15 U.S.C. § 1681p	22
17 U.S.C. § 504(c) (2012)	25
28 U.S.C. § 1715(b)	36
28 U.S.C. § 1715(d)	36

Cal. Civ. Code § 1785.11.2	29
Conn. Gen. Stat. § 42-110m	33
Mass. Gen. Laws ch. 93, § 62A	29
Mass. Gen. Laws ch. 93A, § 4	33
Mass. Gen. Laws ch. 93H, § 3	29
Pub. L. No. 109-2, 119 Stat. 4, § 2(b)(2)	35

RULE

Sup. Ct. R. 37.4	1
------------------------	---

OTHER AUTHORITIES

<i>About</i> , RADARIS, https://radaris.com/page/about ..	14
ACXIOM CORP., FORM 10-K (2015), <i>available at</i> https://www.sec.gov/Archives/edgar/data/733269/000073326915000018/f10k.htm	6
Alessandro Acquisti & Christina M. Fong, <i>An Experiment in Hiring Discrimination Via Online Social Networks</i> (July 18, 2015), <i>available at</i> http://dx.doi.org/10.2139/ssrn.2031979	15
Julia Angwin, <i>The Web's New Gold Mine: Your Secrets</i> , WALL ST. J., July 30, 2010, <i>available at</i> http://www.wsj.com/articles/SB10001424052748703940904575395073512989404	7
Assurance of Discontinuance No. 09-165, <i>In re Choicepoint Workplace Solutions Inc., et al.</i> (Dec. 17, 2009)	18

Assurance of Discontinuance, <i>In re Equifax Info. Serv. LLC, et al.</i> , No. 15-1480E (Mass. Super. Ct. May 20, 2015)	31
Katy Bachman, <i>Big Data Added \$156 Billion in Revenue to Economy Last Year</i> , ADWEEK, Oct. 14, 2014, available at http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107	6
Danielle Keats Citron & Frank Pasquale, <i>The Scored Society: Due Process for Automated Predictions</i> , 89 WASH. L. REV. 1 (2014)	10
<i>CoreLogic SafeRent</i> , CORELOGIC, http://www.corelogic.com/industry/multifamily-housing-solutions.aspx#	13
<i>Credit Risk Assessment</i> , EBUREAU, http://www.ebureau.com/b2c/credit-risk-assessment#credit	12
CROSS-TAB MARKETING SERV. & MICROSOFT CORP., ONLINE REPUTATION IN A CONNECTED WORLD (2010), available at http://download.microsoft.com/download/C/D/2/CD233E13-A600-482F-9C97-545BB4AE93B1/DPD_Online%20Reputation%20Research_overview.doc	15
Pam Dixon & Robert Gellman, <i>The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future</i> , WORLD PRIVACY FORUM (Apr. 2, 2014), available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_Aprill2014_fs.pdf	9

- Enhanced Strategies for Invitation-to-Apply Offers*,
EXPERIAN, <http://www.experian.com/marketing-services/profitability-score.html> 13
- FEDERAL TRADE COMMISSION, DATA BROKERS: A
CALL FOR TRANSPARENCY AND ACCOUNTABILITY,
(2014), *available at* <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> *passim*
- FEDERAL TRADE COMMISSION, REPORT TO CONGRESS
UNDER SECTION 319 OF THE FAIR AND ACCURATE
CREDIT TRANSACTIONS ACT OF 2003 (2012),
available at <https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf> 17
- Forty-Five Percent of Employers Use Social
Networking Sites to Research Job Candidates*
(Aug. 19, 2009), CAREERBUILDER,
<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009> 16
- GOVERNMENT ACCOUNTABILITY OFFICE,
INFORMATION RESELLERS: CONSUMER PRIVACY
FRAMEWORK NEEDS TO REFLECT CHANGES IN
TECHNOLOGY AND THE MARKETPLACE, GAO-13-
663 (2013), *available at* <http://www.gao.gov/assets/660/658151.pdf> 5, 7, 8

Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, <i>Behavioral Advertising: The Offer You Cannot Refuse</i> , 6 HARV. L. & POL'Y REV. 273 (2012)	7
ILLINOIS ATTORNEY GENERAL'S OFFICE, IDENTITY THEFT RESOURCE GUIDE, <i>available at</i> http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf	29
Katie Jennings, <i>How Your Doctor And Insurer Will Know Your Secrets — Even If You Never Tell Them</i> , BUSINESS INSIDER (July 9, 2014), http://www.businessinsider.com/hospitals-and-health-insurers-using-data-brokers-2014-7 . . .	11
Kathy Kristof, <i>Bad Credit Can Double Auto Insurance Premiums</i> , CBS MONEYWATCH (Oct. 25, 2013), http://www.cbsnews.com/news/bad-credit-can-double-auto-insurance-premiums/ . .	12
MASSACHUSETTS ATTORNEY GENERAL'S OFFICE, GUIDE ON IDENTITY THEFT FOR VICTIMS AND CONSUMERS (2015), <i>available at</i> http://www.mass.gov/ago/docs/consumer/id-theft-guide.pdf	28
MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011), <i>available at</i> http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation	5

- Ylan Q. Mui, *Little-Known Firms Tracking Data Used in Credit Scores*, WASHINGTON POST (July 16, 2011), http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_story.html 32
- National Association of Insurance Commissioners, *Credit-Based Insurance Scores*, http://www.naic.org/cipr_topics/topic_credit_based_insurance_score.htm 12
- NATIONAL CONSUMERS LEAGUE, THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH—IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS (2014), *available at* http://www.nclnet.org/datainsecurity_report 27
- Nationwide Employment Background Check*, TALENTWISE, <https://www.talentwise.com/employment-background-check.html?trackit=276> 14
- Nationwide Tenant Background Check*, TALENTWISE, <https://www.talentwise.com/tenant-background-check.html?trackit=278> . . 14
- Frank Pasquale, *Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing*, in THE OFFENSIVE INTERNET—PRIVACY, SPEECH, AND REPUTATION (Levmore, S. & Nussbaum, M. eds. 2010) 16

Martha Poon, <i>Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac and Company Incorporated</i> , 55 SOCIOLOGICAL REVIEW, Sept. 10, 2007	12
Restatement (Second) of Torts § 559	23
Restatement (Second) of Torts § 573	23
Restatement (Second) of Torts § 623A	23
Restatement (Second) of Torts § 652D	23
Restatement (Second) of Torts § 652E	23
Leslie Scism & Mark Maremont, <i>Insurers Test Data Profiles to Identify Risky Clients</i> , WALL ST. J. (Nov. 19, 2010), http://www.wsj.com/articles/SB10001424052748704648604575620750998072986	11
Settlement Agreement, <i>In re Experian Info. Solutions, Inc., Equifax Info. Servs., LLC, & TransUnion LLC</i> (Mar. 8, 2015), available at http://www.ag.ny.gov/pdfs/CRA%20Agreement%20Fully%20Executed%203.8.15.pdf	31
<i>State Security Breach Notification Laws</i> , NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx	32
<i>Tenant Score</i> , MYRENTAL.COM, http://www.myrental.com/products/tenant-score	14

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, MAJORITY STAFF, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES (2013)	<i>passim</i>
<i>Untap New Potential with Underbanked Consumers</i> , EXPERIAN, http://www.experian.com/ marketing-services/data-digest-choicescore.html	13
<i>Why Perform a Background Check?</i> , PEOPLEFINDERS.COM, http://www.peoplefinders. com/background-check	14

INTERESTS OF *AMICI CURIAE*

Amici States¹ file this brief in support of Respondent as a matter of right pursuant to Supreme Court Rule 37.4.

Each of the *Amici* States is charged with protecting the privacy, security, and integrity of its residents' personal data through its enforcement of state and federal consumer protection laws, including the Fair Credit Reporting Act ("FCRA," 15 U.S.C. §§ 1681 *et seq.*) and its state analogues, state unfair or deceptive practices acts, state data breach notification laws, and state data security laws or regulations. These laws prevent and remedy injuries caused to consumers when their personal data is compromised in commerce, whether through security breach, unauthorized disclosure, or inaccuracies.

The *Amici* States seek to ensure that their residents have equal access to opportunities necessary for social and economic well-being, particularly in the areas of credit, employment, housing, and insurance. Increasingly, access to these opportunities is linked to personal data. Accordingly, the *Amici* States share a compelling interest in protecting their residents from suffering harm due to the communication and use of inaccurate personal data in commerce.

Through our enforcement experience, the *Amici* States know that consumers are injured when inaccurate personal data is disseminated to businesses and individuals who rely on this information when

¹ A list of *Amici* States and their counsel appears on the inside cover.

making decisions about those consumers. Through our efforts helping residents mitigate or avoid these harms, we know the time and expense required of consumers to restore the integrity of compromised personal data and have witnessed that many of those efforts are unsuccessful. We have an interest in ensuring that our consumers can redress these injuries when their statutory rights granted by the FCRA are violated.

SUMMARY OF ARGUMENT

New technologies allow for collection, analysis, and dissemination of vast amounts of digital data about consumers. This data is collected by the “data broker” industry. Data brokers amass personal, comprehensive, and detailed information regarding every consumer in the United States. They compile and sell individualized data profiles to a variety of businesses. In turn, businesses use these profiles to make important decisions about consumers regarding credit, employment, housing, and insurance, among others.

Unfortunately, these data profiles frequently contain errors, and when disseminated, propagate false information regarding consumers. These inaccuracies may determine where one is able to work, whether one will be able to rent or buy a home, or whether one will be able to obtain a car loan. However, the damage done by the publication or sale of an inaccurate data profile is frequently impossible for the affected consumer to detect or quantify. Nearly all of the collection, aggregation, disclosure, and use of the data occur without the consumer’s knowledge. Even if a consumer learns of the existence or content of his or her data profile, it is nearly impossible to discover all of the

persons and businesses that have reviewed and relied on the data profile in making decisions affecting the consumer's life. When data brokers communicate inaccurate personal data, affected consumers likely will never know the full extent of the resulting damage.

Congress enacted the FCRA to address the harm caused by the dissemination of inaccurate information about consumers. The statute gives consumers the right to seek redress from data brokers, like Petitioner, who violate the FCRA when communicating and selling inaccurate personal data about them to businesses. In doing so, Congress codified the common-law right to pursue relief for injuries to reputation and property without proof of further harm. By providing this remedy, Congress recognized that the publication of inaccurate data in a consumer report creates a substantial risk of serious adverse consequences for consumers such as: the reasonably foreseeable denial of a mortgage loan; the inability to purchase and insure a vehicle; or the rejection of a job application. Consumers also suffer cognizable harm as a result of the efforts they undertake to mitigate damage from compromised data. These serious injuries more than satisfy the requirements of Article III standing. Because consumers frequently cannot identify or monetize all of the harm caused by inaccurate data profiles, Congress rightly has authorized statutory damages for a willful violation of the FCRA. This private enforcement tool – a vital complement to the enforcement efforts of the *Amici* States – is critical to maintaining consumers' access to opportunities in today's digital economy.

ARGUMENT

I. CONSUMERS ARE ROUTINELY HARMED BY THE DISSEMINATION AND USE OF INACCURATE DATA PROFILES.

An entire industry now exists to collect, aggregate, and sell detailed personal data about each and every one of us. The data that fuels the data broker industry is digital, comprehensive, often quite sensitive, and harvested without our knowledge by numerous entities every day. Once collected, our data is packaged and sold to a variety of companies as purportedly accurate reflections of who we are, who we were, and who we are likely to be. In turn, businesses routinely use these profiles to determine whether we are worthy of credit, employment, housing, or insurance, and, if so, on what terms.

However, decades of experience have demonstrated that consumer data profiles frequently include information that is inaccurate, incomplete, or misleading. Even well-recognized and established consumer data profiles – credit reports – regularly propagate inaccurate consumer data. These mistakes have substantial, everyday consequences for consumers. Yet, the damage done by inaccurate data is nearly impossible to detect or quantify. Even if a consumer identifies and endeavors to correct inaccurate personal data in his or her data profile, he or she may not be aware of all of the adverse decisions already made by specific users of that inaccurate data. Inaccurate data profiles have grave consequences for consumers, but those consequences often remain hidden.

A. Vast Amounts of Detailed, Personal Consumer Data Are Collected, Processed, and Sold By the Data Broker Industry.

New technologies facilitating the rapid collection, analysis, and transfer of digital data about consumers have given rise to the data broker industry.² Data brokers (like Petitioner) “collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling [it] to their customers for various purposes, including verifying an individual’s identity, differentiating records, marketing products, and preventing financial fraud.”³ It is a thriving industry, consisting of hundreds to thousands of companies, and it continues to grow.⁴

² See generally MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

³ See FEDERAL TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at 23-45 (2014) [“FTC DATA BROKER REPORT”], *available at* <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

⁴ See GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE, GAO-13-663, at 5, 34 (2013) [“GAO REPORT”], *available at* <http://www.gao.gov/assets/660/658151.pdf> (estimating between 250 and 2,500 existing data brokers, depending on definition applied, and observing a “vast increase in recent years in the number and type of companies that collect and share [consumers’] data with third parties”); *see also*

The volume and specificity of consumer data compiled by the industry is staggering. One data broker claims to have “[m]ulti-sourced insight into approximately 700 million consumers worldwide” and “[d]emographics, life-stage segmentation, brand affinities, and purchase tendencies for nearly every adult consumer in the U.S.”⁵ Another claims to have “3000 data segments for nearly every U.S. consumer.”⁶

Data brokers rarely interact directly with consumers, but instead gather data from various third-party sources, including: government and public records; social media, online activity, and mobile device usage; retail purchases; and secondary or tertiary (or even more remote) sources, including other data brokers.⁷

Data brokers use various data collection methods, nearly all of which occur without the consumer’s

Katy Bachman, *Big Data Added \$156 Billion in Revenue to Economy Last Year*, ADWEEK, Oct. 14, 2014, available at <http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107>.

⁵ ACXIOM CORP., FORM 10-K at 9 (2015), available at <https://www.sec.gov/Archives/edgar/data/733269/00007332691500018/f10k.htm>.

⁶ See FTC DATA BROKER REPORT at 47.

⁷ See U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, MAJORITY STAFF, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES at 10-11, 15-21 (2013) [“SENATE STAFF REPORT”]; FTC DATA BROKER REPORT at 11-15.

knowledge. Consumer data is collected when consumers use applications on their smartphones or tablets, or in the case of geolocation data,⁸ just by carrying such devices in their pockets.⁹ Consumers' interactions with websites (e.g., search requests, sites visited, links clicked, and purchases made) are tracked and collected by any number of companies using "cookies,"¹⁰ "flash cookies" (which resist consumers' efforts to delete them), or "history sniffers" (which collect web browsing history).¹¹ Consumer data is also harvested in bulk from the internet using "web scrapers," technology that scans various online sources to collect data reflecting a consumer's activity or

⁸ "Geolocation data" indicates a mobile device's physical location.

⁹ See GAO REPORT at 24-27.

¹⁰ A "cookie" is a text file placed on a computer when a user visits a website. See Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012).

¹¹ See GAO REPORT at 23-24 (describing various online tracking technologies); see also Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1, available at <http://www.wsj.com/articles/SB10001424052748703940904575395073512989404> (finding top 50 websites in the nation, representing approximately 40% of websites viewed by Americans, installed average of 64 pieces of tracking technology onto visitors' computers, often without warning, to scan and collect, in real-time, a visitor's website activity); see generally Hoofnagle, *et al.*, *supra* note 10 (outlining internet tracking technologies).

postings on social media, blogs, and even other data broker websites.¹²

Nearly all of this data collection occurs outside of consumers' control, knowledge, or view. In 2012, prompted by concerns of consumer harm, the Majority Staff of the U.S. Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, studied the data broker industry. Based on its inquiry, it concluded:

[C]onsumers going about their daily activities – from making purchases online and at brick-and-mortar stores, to using social media, to answering surveys to obtain coupons or prizes, to filing for a professional license – should expect that they are generating data that may well end up in the hands of data brokers[;] that this data may well be amassed with many other details about them data brokers already have compiled[; and] that data brokers will draw on this data without their permission to construct detailed profiles on them reflecting judgments about their characteristics and predicted behaviors.¹³

¹² See GAO REPORT at 18; FTC DATA BROKER REPORT at 17 (observing that “some data brokers collect publicly available web-based data through web crawlers, which are programs that capture content across the Internet and transmit it back to the data broker’s servers”).

¹³ SENATE STAFF REPORT at 35.

The data collected is detailed, personal, and often sensitive. In addition to demographic information, data brokers track, *inter alia*:

- financial and health status;
- hobbies;
- religious and political affiliations;
- stores visited, shopping habits, and items purchased;
- geolocation;
- online and social media activity;
- financial transactions;
- books read, movies or television shows watched, and music listened to;
- sexual habits and/or orientation;
- type of device used to access the internet; and
- grocery and alcohol purchases.¹⁴

Data brokers also make and record in a consumer's data profile inferences from raw data (e.g., that a

¹⁴ See *id.* at 13-15 (showing variety of information collected by data brokers, including, e.g., whether consumer purchases particular shampoo or soft drink; miles traveled in prior weeks; alcoholic beverages consumed, whether consumer owns pets, hunts, maintains juvenile life insurance, or suffers from ailments such as Attention Deficit Hyperactivity Disorder); FTC DATA BROKER REPORT at 11-14 (listing variety of data elements collected by nine data brokers subject to the FTC's inquiry); Pam Dixon & Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*, WORLD PRIVACY FORUM (Apr. 2, 2014), at 33-38, available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April12014_fs.pdf (listing 187 exemplar types of data elements, and numerous subtypes, used to generate various consumer scores, including information relating to vehicle ownership, lifestyle, interests, activities, medical status, property, and assets).

consumer is a parent based on purchase of baby products). They may also aggregate several raw data points to create new data points, including various “scores” that purport to rate consumers according to attributes considered favorable or unfavorable or predict future behavior or tendencies.¹⁵

Data brokers also use consumer data to group consumers into categories based on perceived identity, behavior, socio-economic status, or other commonalties.¹⁶ Such segments include, for example, categories labeled “Urban Scramble” or “Mobile Mixers” (referring to segments including high concentrations of Latino and African-American consumers), “Thrifty Elders” (including singles in their late 60’s and early 70’s in “one of the lowest income clusters”), “Working Class Mom,” “Modest Wages,” or “Financially Challenged.”¹⁷

Data brokers market these consumer data profiles to businesses across many industries as purportedly accurate proxies for a consumer’s identity, socio-

¹⁵ See generally, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014). Examples of some consumer scores are also described *infra*, Section I.B.

¹⁶ See SENATE STAFF REPORT at 21-28 (describing various consumer profiles offered by data brokers); FTC DATA BROKER REPORT at 19-21 (same).

¹⁷ FTC DATA BROKER REPORT at 19-21. See also SENATE STAFF REPORT at 24 (other segments also focus on a consumer’s perceived economic status, including “American Royalty,” “Power Couples,” “Established Elite,” “Mid-Life Strugglers,” “Credit Reliant,” or “Zero Mobility”).

economic status, or interests. They also market the profiles as reliable predictors of a consumer's future behavior – including whether a consumer will buy a particular product, respond to a particular sales offer, default on a loan, or be a good insurance risk, tenant, or employee.

B. Businesses Frequently Rely on Data Profiles to Make Decisions With Important Consequences for Consumers.

While the commercial use of consumer data profiles is not new, emerging technologies and the digitization of data have dramatically expanded the volume and commercial availability of ever-more detailed data. Businesses now have near-instant access to volumes of data about consumers, on which they rely to make decisions about whether and which products (and on what terms) to offer to consumers.

Insurance companies rely on a wide range of data about consumers to screen out potential “high risk” individuals. Life and health insurers pull data from data brokers' databases to analyze a consumer's shopping habits, exercise interests, and online searches on the theory that such data points are accurate proxies for underwriting risks.¹⁸ Similarly, where not prohibited by state law, auto insurers use credit scores

¹⁸ See Katie Jennings, *How Your Doctor And Insurer Will Know Your Secrets — Even If You Never Tell Them*, BUSINESS INSIDER (July 9, 2014), <http://www.businessinsider.com/hospitals-and-health-insurers-using-data-brokers-2014-7>; Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J. (Nov. 19, 2010), <http://www.wsj.com/articles/SB10001424052748704648604575620750998072986>.

as a proxy to identify “high risk” consumers for whom the insurers set higher rates (in some cases up to 116% more on average).¹⁹

In addition to the more widely-known FICO® score,²⁰ lenders now rely on new generations of consumer “scores” created by data brokers to identify credit-worthy consumers. Data brokers create such scores by conglomerating various data points about a consumer into a number that purports to accurately predict a consumer’s future behavior. They include, for example, “eScores” that claim to allow “companies to effectively segment credit risks” with respect to “consumers who do not have a scoreable [*sic*] credit file with the major credit reporting agencies.”²¹ Similarly,

¹⁹ Kathy Kristof, *Bad Credit Can Double Auto Insurance Premiums*, CBS MONEYWATCH (Oct. 25, 2013), <http://www.cbsnews.com/news/bad-credit-can-double-auto-insurance-premiums/>. See also National Association of Insurance Commissioners, *Credit-Based Insurance Scores* (last updated Feb. 27, 2015), http://www.naic.org/cipr_topics/topic_credit_based_insurance_score.htm (noting prevalence of use of consumer credit information in homeowner or auto insurance underwriting, and observing that “FICO estimates approximately 95% of auto insurers and 85% of homeowners’ insurers use credit-based insurance scores in states where it is a legally allowed underwriting or risk classification factor”).

²⁰ The FICO® score was developed by Fair, Isaac & Co. in 1956 to predict the likelihood of a consumer defaulting on a debt. See generally Martha Poon, *Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac and Company Incorporated*, 55 SOCIOLOGICAL REVIEW, Sept. 10, 2007.

²¹ *Credit Risk Assessment*, EBUREAU, <http://www.ebureau.com/b2c/credit-risk-assessment#credit> (last visited Sept. 8, 2015).

the “ChoiceScoreSM” is marketed as a way to “help[] marketers identify and more effectively market to underbanked consumers,” such as “[n]ew legal immigrants,” “recent graduates,” “widows,” or “[c]onsumers with transitory lifestyles, such as military personnel.”²² The “Consumer View Profitability Score” offers “13 levels with three high-profitability levels” to enable businesses to “select[] the best prospects that will respond and comply with the terms of their Invitation-to-Apply lending, credit, or continuity program offers.”²³

Landlords and employers use “on demand” consumer data profiles to quickly evaluate prospective tenants or employees. One data broker offers landlords access to “superior data and screening technology [to] help [them] lease to the right people,” including “comprehensive data about evictions, address[] history, criminal and additional proprietary sources” that “help [them] evaluate the risk of a resident and make a quick decision to fill [their] rental properties.”²⁴ Another offers “the most comprehensive on-demand background check available today” to evaluate prospective

²² *Untap New Potential with Underbanked Consumers*, EXPERIAN, <http://www.experian.com/marketing-services/data-digest-choicescore.html> (last visited Sept. 8, 2015).

²³ *See Enhanced Strategies for Invitation-to-Apply Offers*, EXPERIAN, <http://www.experian.com/marketing-services/profitability-score.html> (last visited Sept. 8, 2015).

²⁴ *See CoreLogic SafeRent*, CORELOGIC, <http://www.corelogic.com/industry/multifamily-housing-solutions.aspx#> (last visited Sept. 8, 2015).

employees or tenants.²⁵ To further expedite tenant screening, three-digit “tenant scores” that purport to “summarize[] the potential risk of the applicant compared to others” are also available.²⁶

Many data brokers, like Petitioner, offer “people search” websites, which they market as an efficient and low-cost (or even free) resource for conducting background screens. For example, one data broker provides an on-line “universal people directory and an information indexing system” containing data pulled from “social media, official public records, publications and user reviews” to “allow[] people to get to know each other and their professional reputation prior to establishing a relationship.”²⁷ Another similar website offers a “Comprehensive Background Check” that reveals “if anyone has a bankruptcy or criminal charges in their history,” and advertises “the most detailed reports available to provide security for you, your business and your loved ones.”²⁸ Petitioner specifically

²⁵ See *Nationwide Employment Background Check*, TALENTWISE, <https://www.talentwise.com/employment-background-check.html?trackit=276> (last visited Sept. 8, 2015); *Nationwide Tenant Background Check*, TALENTWISE, <https://www.talentwise.com/tenant-background-check.html?trackit=278> (last visited Sept. 8, 2015).

²⁶ See *Tenant Score*, MYRENTAL.COM, <http://www.myrental.com/products/tenant-score> (last visited Sept. 8, 2015).

²⁷ See *About*, RADARIS, <https://radaris.com/page/about> (last visited Sept. 8, 2015).

²⁸ See *Why Perform a Background Check?*, PEOPLEFINDERS.COM, <http://www.peoplefinders.com/background-check> (last visited Sept. 8, 2015).

targets employers, inviting those “looking to hire someone” to turn to “Spokeo free people search [a]s a great research tool to learn more about prospective ... employees.” JA 13 (at ¶ 28).

Particularly for employers, online consumer data provides a tempting shortcut to the traditional application process, offering a way to quickly winnow stacks of resumes. A 2010 survey co-authored by Microsoft found that 98% of the 275 U.S. employers surveyed searched various websites for information to evaluate candidates, with 32% specifically searching websites that aggregate personal data about applicants.²⁹ Indeed, 75% of those employers considered online data so important that they imposed formal policies mandating hiring personnel to research applicants online.³⁰ According to a 2015 Carnegie Mellon University study, about one-third of U.S. firms searched online social networks for information about job applicants early in the hiring process, and made hiring decisions based on the search results.³¹

²⁹ CROSS-TAB MARKETING SERV. & MICROSOFT CORP., ONLINE REPUTATION IN A CONNECTED WORLD 8 (2010), *available at* http://download.microsoft.com/download/C/D/2/CD233E13-A600-482F-9C97-545BB4AE93B1/DPD_Online%20Reputation%20Research_overview.doc.

³⁰ *Id.* at 6.

³¹ Alessandro Acquisti & Christina M. Fong, *An Experiment in Hiring Discrimination Via Online Social Networks* (July 18, 2015), *available at* <http://dx.doi.org/10.2139/ssrn.2031979> (finding “that about one third of employers likely searched online for the candidates’ information” and that results of those searches resulted in religious-based bias in certain geographic areas).

Online data about an employment applicant can directly affect whether the applicant will be interviewed or hired. According to a 2009 survey of over 2,600 hiring managers, 45% used social networking sites to research job candidates, with 35% of those employers deciding not to hire candidates based on information they learned through that research. Of that group, 24% disregarded a candidate after obtaining information online suggesting that the candidate was lying about his qualifications.³²

C. Error-Prone Consumer Data Profiles Lead to Negative Consequences that Consumers Are Unable to Identify.

Consumer reports have been maintained for decades and, for just as long, have contained erroneous or misleading information. In addition to straightforward inaccuracies, early credit reports also contained speculative innuendo analogous to contemporary internet gossip (e.g., a consumer “used ‘his hands in an effeminate manner, also talks in an effeminate manner’”).³³ Because these reports drove denials of access to credit, employment, housing, and insurance, Congress enacted the FCRA in 1970.

³² *Forty-Five Percent of Employers Use Social Networking Sites to Research Job Candidates* (Aug. 19, 2009), CAREERBUILDER, <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009> (last visited Sept. 8, 2015).

³³ Frank Pasquale, *Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing*, in *THE OFFENSIVE INTERNET—PRIVACY, SPEECH, AND REPUTATION*, at 111 & n.13 (Levmore, S. & Nussbaum, M. eds. 2010).

Yet, even today, consumer reports continue to propagate inaccurate information. According to a 2012 FTC study, approximately one in four consumers encountered one or more errors in at least one of the credit reports issued by the three national credit reporting bureaus (Equifax, Experian, and TransUnion).³⁴ The errors identified by the consumers could “potentially change the credit score associated with that credit report.”³⁵ Even the reports of the national credit reporting bureaus – which have long been subject to the FCRA – continue to contain errors. In contrast, many data brokers, like Petitioner, expressly disclaim any obligation to comply with the FCRA (*see* JA 19-20 (at ¶ 56)) and may not maintain any formal policies to allow consumers to correct errors in their data profiles. Lacking even the modest safeguards required by the FCRA, data broker profiles are likely to contain even more inaccuracies than credit reports.

The experience of the *Amici* States echoes the FTC’s findings. Our consumers encounter numerous inaccuracies in their credit reports and online data profiles including: incorrect address or age; a

³⁴ *See* FEDERAL TRADE COMMISSION, REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 at i (2012), *available at* <https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf>.

³⁵ *Id.*

misattributed criminal record;³⁶ wrong employer; or business complaints related to another person or company. Data profiles are frequently inaccurate due to identity theft.

Despite the grave consequences that false data profiles carry for consumers, the scope of the damage often remains hidden from them. As the Senate Committee observed, “data brokers ... provide consumers rights of access and control regarding their data that vary widely.”³⁷ Indeed, this “fundamental lack of transparency” coupled with the risk of resulting harms to consumers prompted the FTC to recommend legislation “that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by th[o]se entities.”³⁸

Accordingly, identifying the negative consequences of an inaccurate data broker profile can be a difficult – and possibly insurmountable – burden for a consumer. An employer may reject a candidate based on a glance at a data broker’s website without the candidate ever knowing. The FTC described this quandary: “if a

³⁶ See Assurance of Discontinuance No. 09-165, *In re Choicepoint Workplace Solutions Inc., et al.* (Dec. 17, 2009) (resolving investigation by the New York Attorney General’s Office and requiring consumer reporting agency to ensure accurate reporting of criminal records of job applicants to prospective employers), available at http://www.ag.ny.gov/sites/default/files/pdfs/bureaus/civil_rights/ChoicePoint%20AOD.pdf.

³⁷ SENATE STAFF REPORT at 12.

³⁸ FTC DATA BROKER REPORT at 49.

consumer is denied the ability to conclude a transaction based on an error in a [consumer report], the consumer can be harmed without knowing why.”³⁹

Even if a consumer discovers inaccuracies in his or her data profile maintained by an identifiable data broker – a daunting task itself, given the sheer number of data brokers (many of which do not reveal their data for free) – it can be difficult, if not impossible, for the consumer to trace the flow of the inaccurate information through various users and connect it to the consequences. And while a consumer may strongly suspect that inaccurate information disseminated by an identified data broker was the basis for a specific adverse decision, proving that the decision-maker actually viewed and was influenced by that data is even more challenging.

II. THE FCRA IS A CRITICAL TOOL TO PROTECT CONSUMERS FROM THE DISSEMINATION OF INACCURATE DATA PROFILES.

The FCRA serves a vital purpose – one even more critical now than when it was first enacted in 1970. Even before the advent of the internet, Congress recognized the development of an “elaborate mechanism ... for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.” 15 U.S.C. § 1681(a)(2). This necessitated legislation “to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and

³⁹ *Id.* at 48.

a respect for the consumer’s right to privacy.” *Id.* § 1681(a)(4). In the ensuing 45 years, the “elaborate mechanism[s]” Congress described have evolved into digital algorithms that can aggregate and analyze vast amounts of consumer data to create even more detailed consumer reports, accessible through the internet to anyone at the click of a button. Against this backdrop, the FCRA’s procedural and substantive protections, especially those requiring consumer reporting agencies to “follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual,” have never been more necessary. *Id.* § 1681e(b).

Consumers need to have the ability to enforce these protections, notwithstanding their difficulties in showing actual damages. The FCRA recognizes that the dissemination of inaccurate consumer information creates a substantial risk of harm, though specific harms are often hard to identify or quantify. In addition, common-law has long protected against damage to reputational or property interests, even without proof of actual injury. Courts also have recognized as sufficient for Article III standing the cost of mitigating the substantial risk of injury due to the dissemination of personal information in the analogous context of a data security breach. If anything, similar and possibly greater cost and effort are required to correct inaccurate information communicated by a data broker.

A. The FCRA Is Intended to Protect Consumers Against the Dissemination of Inaccurate Data Profiles by Data Brokers.

The express purpose of the FCRA is to ensure that “consumer reporting agencies,” a term defined to include entities like Petitioner,⁴⁰ act responsibly in the “vital role” they have assumed. 15 U.S.C. § 1681(a)(3). The FCRA requires that these agencies adopt minimum “reasonable procedures” that “meet[] the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information[.]” *Id.* § 1681(b).

By definition, a consumer report is “any ... communication ... bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for” a number of enumerated purposes. *Id.* § 1681a(d)(1). Congress created a right for an individual to be free from a credit reporting agency’s willful dissemination of inaccurate information in a consumer report. *See id.* §§ 1681e(b), 1681a(d). The FCRA imposes civil liability for that

⁴⁰ “Consumer reporting agenc[ies]” include any person or entity “which, for monetary fees, dues, or on a cooperative nonprofit basis, 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[.]” 15 U.S.C. § 1681a(f).

dissemination when the agency willfully fails to employ “reasonable procedures to assure maximum possible accuracy” of the information contained therein. *Id.* §§ 1681e(b), 1681n. Congress also gave consumers the right to seek redress in federal court for violations of such requirements. *Id.* §§ 1681n, 1681o, 1681p.

Thus, through the FCRA, Congress recognized the substantial risk of harm to a consumer, albeit often difficult to quantify or prove, when inaccurate information about a consumer is willfully communicated for the purpose of evaluating his or her eligibility for, *inter alia*, credit, employment, or insurance. *See id.* §§ 1681a(d)(1), 1681b(a). Congress made the integrity of a consumer’s personal data profile a legally enforceable right and provided a means for redress when inaccurate data is inappropriately shared, collected, or used for important decisions.

The purpose of the FCRA is to protect against the exact conduct at issue in this case – the dissemination of inaccurate profiles describing “a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.” *Id.* § 1681a(d)(1). The FCRA is thus an important tool to protect consumers from abuses by the data broker industry.

**B. Harm to Reputation or Property Rights,
Even Without Proof of Additional Injury,
Has Been Long Understood to Create a
Judicable Case.**

The injuries resulting from the communication and use of inaccurate personal data are real, particularized, and concrete. It is precisely because of these injuries

that Congress gave consumers the right to seek redress when a consumer reporting agency violates the FCRA's procedural safeguards. Through the FCRA, Congress has exercised its authority to "elevat[e] to the status of legally cognizable injur[y]" these "concrete, *de facto* injuries that were previously inadequate in law[.]"⁴¹ *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992).

The *de facto* injuries that Congress has recognized in the FCRA have strong "analogs in our common-law tradition." *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring). The publication of false information can be sufficient to establish standing for traditional common-law defamation claims designed to vindicate reputational injury that can impact one's livelihood. See, e.g., Restatement (Second) of Torts § 573 (Defamation Actionable Irrespective of Special Harm (Defamation Actionable *Per Se*)) (statement ascribing to another characteristics or conduct that would adversely affect his fitness for, *inter alia*, "the proper conduct of his lawful business, trade or profession," subjects speaker to liability "without proof of special harm").⁴² This Court has recognized that such claims

⁴¹ The *Amici* States do not elaborate here on the broader question of whether the violation of any statutory right can, standing alone, suffice to establish cognizable Article III standing. This Court need not reach that question here given the concrete, consequential injuries caused by the dissemination of inaccurate personal data.

⁴² See also Restatement (Second) of Torts § 559 (1977) (defamatory communications), § 623A (publication of injurious falsehood), § 652D (publicity given to private life), § 652E (publicity placing person in false light).

– allegations of injury by published falsehoods that specifically concern the individual – are “of the sort traditionally amenable to, and resolved by, the judicial process.” *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 102 (1998); *see also Meese v. Keene*, 481 U.S. 465, 474-75 (1987) (holding that “a risk of injury to [one’s] reputation” is sufficient injury for Article III standing). Consumer reports are dossiers of our lives – reputational summaries detailing our past educational, financial, purchasing, residential, and social histories – that are routinely used in making judgments that will affect our futures. In effect, Congress, through the FCRA, has elevated and codified the *de facto* common-law right to be free from the publication of false information in the specific context of consumer reports.

Moreover, the common-law has always recognized the right to control one’s property without regard to quantifiable harm. Common-law actions for trespass have long vindicated real property rights without proven physical damage,⁴³ and patent and copyright infringement actions similarly protect intangible intellectual property without the requirement to allege or prove economic damage.⁴⁴ Violations of tangible and

⁴³ *See, e.g., Marzetti v. Williams*, 1 B. & Ad. 415, 426, 109 Eng. Rep. 842, 846 (K.B. 1830) (Taunton, J.) (“Trespass, *quare clausum fregit*, is maintainable for an entry on the land of another, though there be no real damage, because repeated acts of going over the land might be used as evidence of a title to do so, and thereby the right of the plaintiff may be injured.”).

⁴⁴ *See, e.g., Rude v. Westcott*, 130 U.S. 152, 167 (1889) (awarding nominal damages where “[n]o legal ground [was] shown for the recovery of specific damages for the alleged infringement of the

intangible property rights are actionable without a showing of damages or harm because the violations are themselves injuries-in-fact. Just as the value of real or intangible property derives in part from the extent to which its owner can exercise control over it, Congress sought through the FCRA to protect a consumer's interest in controlling the integrity of his information – which also has marketable value⁴⁵ – when it is

patents”); *Whittemore v. Cutter*, 29 F. Cas. 1120, 1121 (C.C.D. Mass. 1813) (Story, J.) (holding that patent owner could recover nominal damages from defendant who infringed his patent because, “where the law gives an action for a particular act, the doing of that act imports of itself a damage to the party. Every violation of a right imports some damage, and if none other be proved, the law allows a nominal damage.”); *see also* the Copyright Act, 17 U.S.C. § 504(c) (2012) (providing statutory damages for copyright infringement without proof of other injury); *Feltner v. Columbia Pictures Television, Inc.*, 523 U.S. 340, 341 (1998) (observing “close 18th-century analogues to [17 U.S.C.] § 504(c) statutory damages actions,” including “the common law and statutes in England and this country [which] granted copyright owners causes of action for infringement”); *F.W. Woolworth Co. v. Contemporary Arts, Inc.*, 344 U.S. 228, 233 (1952) (“Even for uninjurious and unprofitable invasions of copyright the court may, if it deems it just, impose a liability within statutory limits to sanction and vindicate the statutory policy.”).

⁴⁵ *See, e.g. Tyler v. Michaels Stores, Inc.*, 464 Mass. 492, 504 n.20 (2013) (concluding that “receipt of unwanted marketing material” due to merchant’s collection of personal information in violation of state law was an “invasion of the consumer’s personal privacy causing injury or harm” that warranted damages equal to the merchant’s profits from use of the information – “a close approximation of the value of the consumer’s personal identification information on the open market”). Indeed, consumer reporting agencies by definition furnish reports on individuals “for

communicated in a consumer report.⁴⁶ See 15 U.S.C. §§ 1681e(b), 1681a(d)(1), 1681b(a).

C. The Dissemination of Inaccurate Personal Data Causes a Substantial Risk of Injury Sufficient for Standing.

Congress recognized that the dissemination of inaccurate personal data creates a substantial risk of injury in the form of adverse decisions relating to, *inter alia*, “credit[,] insurance” or “employment.” 15 U.S.C. §§ 1681a(d), 1681b. Thus, when a company fails to use “reasonable procedures” when “prepar[ing] a consumer report” “with respect to any [given] consumer,” the FCRA creates a cause of action in favor of “that consumer.” *Id.* §§ 1681e(b), 1681n(a). The FCRA “does not require a consumer to wait for unreasonable credit reporting procedures to result in the denial of credit or other consequential harm before enforcing [his or her] statutory rights.” *Beaudry v. Telecheck Services*, 579 F.3d 702, 705 (6th Cir. 2009). Nor should it.

Standing does “not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about.” *Clapper v. Amnesty Int’l USA*, __ U.S. __, 133 S. Ct. 1138, 1150 n.5 (2013).

monetary fees, dues, or on a cooperative nonprofit basis.” 15 U.S.C. § 1681a(f).

⁴⁶ Last term, this Court decided a case involving the denial of an individual’s statutorily-conferred right to control the integrity of his personal data (specifically, his birthplace) listed on a passport, without explicitly considering the jurisdictional question of whether his injury was sufficient to establish Article III standing. *Zivotofsky v. Kerry*, __ U.S. __, 135 S. Ct. 2076 (2015).

Rather, in some circumstances, as here, a “substantial risk” that the harm will occur, “which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm,” suffices to establish standing. *Id.*

In a parallel context involving the compromise of consumers’ personal information as a result of a data security incident or “data breach” by criminal intrusion, courts have concluded that “customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing[.]” *Remijas v. Neiman Marcus Group, LLC*, Dkt. No. 14-3122, 2015 WL 4394814, at *4 (7th Cir. July 20, 2015) (citing *Clapper*, 133 S. Ct. at 1147); see also *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (“*Adobe*”) (also applying *Clapper*’s “certainly impending” harm standard). Since hackers “deliberately targeted” the defendants in order to obtain plaintiffs’ credit-card information, “[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.” *Neiman Marcus*, 2015 WL 4394814, at *5; see *Adobe*, 66 F. Supp. 3d at 1214 (“[T]he risk that Plaintiffs’ personal data will be misused by the hackers who breached Adobe’s network is immediate and very real.”). Recognizing that such harms “can occur long after a data breach,”⁴⁷ the courts in *Neiman Marcus* and *Adobe* held that it is “plausible

⁴⁷ Breach of a Social Security number can increase a consumer’s risk of identity theft 18 times. See NATIONAL CONSUMERS LEAGUE, THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH–IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS 14 (2014), available at http://www.nclnet.org/datainsecurity_report.

to infer that the plaintiffs have shown a substantial risk of harm” from the data breach, and that such allegations of future injury satisfy Article III. *Neiman Marcus*, 2015 WL 4394814, at *5; *see Adobe*, 66 F. Supp. 3d at 1215 (“[T]he danger that Plaintiffs’ stolen data will be subject to misuse can plausibly be described as ‘certainly impending.’”).⁴⁸

These same courts have found that mitigation expenses to protect against such reasonably imminent harms also “qualif[y] as a concrete injury.” *Neiman Marcus*, 2015 WL 4394814, at *5; *see Adobe*, 66 F. Supp. 3d at 1217 (“[I]n order for costs incurred in an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm being mitigated must itself be imminent.”). Indeed, in the data breach context, efforts and costs to restore the security of one’s compromised personal data and avoid identity theft are not insubstantial. The *Amici* States commonly advise consumers⁴⁹ to place and pay for security freezes on

⁴⁸ *See also Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (holding, pre-*Clapper*, that Starbucks employees alleged “a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data” and that, as a result, they “sufficiently alleged an injury-in-fact for purposes of Article III standing”). As the *Adobe* Court observed, a number of district courts, post-*Clapper*, have concluded that plaintiffs lacked standing in similar contexts when applying a heightened “certainly impending” future injury standard. *See Adobe*, 66 F. Supp. 3d at 1212-16 (evaluating *Clapper*’s dual standards, collecting and distinguishing cases, and finding sufficient injury under both standards).

⁴⁹ *See, e.g.*, MASSACHUSETTS ATTORNEY GENERAL’S OFFICE, GUIDE ON IDENTITY THEFT FOR VICTIMS AND CONSUMERS (2015), *available at* <http://www.mass.gov/ago/docs/consumer/id-theft-guide.pdf>;

their credit reports to prevent identity thieves from opening new lines of credit;⁵⁰ to file police reports;⁵¹ to place fraud alerts on their credit files (to obtain early warning of new accounts being opened in their name); to pay for credit-monitoring services; to contact fraud departments at their financial institutions and dispute fraudulent charges to avoid being held responsible for them; to close and reopen compromised financial accounts; to change user names and passwords for compromised accounts; and to change the compromised personal information (e.g., obtain new drivers' license numbers or Social Security numbers⁵²). Some of these prophylactic steps have associated costs, and all require time and effort and compound the emotional distress of living in a state of heightened alert for identity theft or fraud. As courts have found and as the *Amici* States can attest, these attendant injuries are

ILLINOIS ATTORNEY GENERAL'S OFFICE, IDENTITY THEFT RESOURCE GUIDE, *available at* http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf.

⁵⁰ *See, e.g.*, Mass. Gen. Laws ch. 93, § 62A (requiring credit reporting agencies to freeze consumers' credit files upon request and setting a maximum fee of \$5 for each placement, temporary suspension, and lift of such freeze); Cal. Civ. Code § 1785.11.2 (same, with a maximum fee of \$10).

⁵¹ *See, e.g.*, Mass. Gen. Laws ch. 93H, § 3 (requiring breached entities to inform consumers of their right to file and obtain a police report).

⁵² The steps required to change one's Social Security Number following identity theft are detailed at <https://faq.ssa.gov/link/port al/34011/34019/Article/3789/Can-I-change-my-Social-Security-number>.

also real and concrete. *See Neiman Marcus*, 2015 WL 4394814, at *5 (holding that purchase of credit-monitoring services at \$4.95 for first month, and \$19.95 per month thereafter, “easily qualifies as a concrete injury”); *Adobe*, 66 F. Supp. 3d at 1216-17 (concluding that plaintiffs “adequately alleged that they face a certainly impending future harm from the theft of their personal data,” and that “the costs ... incurred to mitigate this future harm [including paying for data monitoring services] constitute an additional injury-in-fact”).

A similar “substantial risk” of harm exists where consumer reporting agencies disseminate consumer data while failing to maintain the “maximum possible accuracy” of that information. 15 U.S.C. § 1681e(b). Like hackers in the data breach context, third parties deliberately request and pay for the targeted individual’s consumer report. The purpose of obtaining a consumer report is, sooner or later, to make a significant decision regarding the consumer based on the purchased personal data. Even supposedly “favorable” inaccuracies can lead to harmful misjudgments when, for example, a consumer is deemed overqualified for a job, ineligible for a needs-based government benefit, or perceived to be untruthful based on contrary information in a consumer report. These determinations may not be immediately apparent or even knowable by a consumer. This is especially true in the case of data brokers (like Petitioner) that disseminate inaccurate

consumer data through a publicly available website to be viewed anonymously by any number of parties.⁵³

Even when a consumer does learn that inaccurate personal information has been disseminated in a consumer report, significant time and effort is required to attempt to identify the source of such errors and to correct them, often to no avail. The *Amici* States have worked with numerous consumers concerned that misleading information has been collected about them by online data brokers, like Petitioner. The process to remove or correct such inaccurate data frequently involves repeated telephone calls, letters, emails, collection and submission of authenticating identification documents, and payment of fees, even when *Amici* States' Attorneys General intervene. Often, despite such efforts, the data broker refuses to give consumers access to their personal data or to correct the inaccuracies, and inaccurate personal data

⁵³ Indeed, consumer complaints of inaccurate credit reporting and concerns that those practices were resulting in lost credit, employment, housing, and insurance opportunities for consumers, among other concerns, prompted many of the *Amici* States to investigate the practices of the three major credit reporting bureaus. That investigation resolved by an Assurance of Voluntary Compliance, enforceable by thirty-one States, which required the credit reporting bureaus to, *inter alia*, implement various measures to improve credit report data accuracy and dispute procedures. See, e.g., Assurance of Discontinuance, *In re Equifax Info. Serv. LLC, et al.*, No. 15-1480E (Mass. Super. Ct. May 20, 2015). The New York Attorney General's Office reached a separate agreement with the three bureaus that included similar provisions. See Settlement Agreement, *In re Experian Info. Solutions, Inc., Equifax Info. Servs., LLC, & TransUnion LLC* (Mar. 8, 2015) available at <http://www.ag.ny.gov/pdfs/CRA%20Agreement%20Fully%20Executed%203.8.15.pdf>.

is republished even after consumers request corrections.

Compared to the mitigation efforts consumers must make when victimized by a data breach, the efforts required to restore the integrity of personal data compromised by a consumer reporting agency can be significantly more challenging. Data brokers obtain a wide variety of data about consumers from various sources, including other data brokers, and then make that information available to any number of anonymous users through the internet. Even if a consumer determines which data broker maintains inaccurate personal data about him or her – which is no small feat⁵⁴ – he or she will not readily know where the broker obtained it, and with whom it has been shared.⁵⁵ To prevent further dissemination of

⁵⁴ In contrast, consumers in most states receive statutory notice from a specific company when their personal information is compromised in a security breach. *See State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (last visited Sept. 8, 2015).

⁵⁵ *See* Ylan Q. Mui, *Little-Known Firms Tracking Data Used in Credit Scores*, WASHINGTON POST (July 16, 2011), http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_story.html (noting “veil of secrecy surrounding the origins of the information [in a consumer data profile], how it is analyzed and who buys it” and observing that “[c]onsumers have no voice in those decisions, even though the information concerns their lives[,]” and that it can also “penalize them for actions they didn’t realize were being tracked, forcing them to pay far higher interest rates or more fees”).

inaccurate personal data, however, a consumer must trace the inaccurate data through possibly still other data brokers and finally to the business entities to which it was disseminated and then correct the erroneous information at each step. These efforts require substantial expenditures of time, energy, and resources – additional real and concrete injuries, albeit hard to monetize – and, in the end, may be wholly unsuccessful.

D. Statutory Damages Cases and Private Class Actions Are Needed to Complement the Role of Attorneys General in Protecting Consumers.

As noted above, the “fundamental lack of transparency” characterizing the data broker industry means that it is frequently impossible for a consumer to know the concrete harm caused by the dissemination of inaccurate personal data.⁵⁶ Appropriately, the FCRA places the burden of ensuring “maximum possible accuracy” on consumer reporting agencies. 15 U.S.C. § 1681e(b). To require otherwise would set an unreasonably high bar that consumers could only rarely overcome.⁵⁷

⁵⁶ FTC DATA BROKER REPORT at 49.

⁵⁷ Of course, because of the substantial public and quasi-sovereign interests at stake, the State Attorneys General are not subject to the same Article III standing limitations as private litigants, and may bring actions under their respective state’s consumer protection laws without waiting for their consumers to be injured or having to prove harm. *See Mass. v. Envtl. Prot. Agency*, 549 U.S. 497, 516-526 (2007); *see also* Mass. Gen. Laws ch. 93A, § 4; Conn. Gen. Stat. § 42-110m.

The statutory damages provided in Section 1681n(a)(1)(A) compensates individuals for actual harm resulting from a willful FCRA violation that is hard to identify, monetize, or otherwise quantify. “That [the] actual loss is small and hard to [identify or] quantify is why statutes such as the [FCRA] provide for modest damages without proof of injury.” *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 953 (7th Cir. 2006); *see also Bateman v. American Multi-Cinema*, 623 F.3d 708, 718 (9th Cir. 2010) (stating, in context of Fair and Accurate Credit Transactions Act (“FACTA”), which incorporates FCRA’s statutory damages provision: “The need for statutory damages to compensate victims is plain. The actual harm that a willful violation of FACTA will inflict on a consumer will often be small or difficult to prove.”). “That Congress provided a consumer the option of recovering either actual or statutory damages, but not both, supports the presumption that they serve the same purpose.” *Bateman*, 623 F.3d at 718 (noting further that Congress’s provision for punitive damages in 15 U.S.C. § 1681n(a)(2) in addition to any actual or statutory damages “suggests that the statutory damages provision has a compensatory, not punitive, purpose”); *see also Harris v. Mexican Specialty Foods, Inc.*, 564 F.3d 1301, 1313 (11th Cir. 2009) (concluding that, because FCRA, which is incorporated into FACTA, provides separately for punitive damages, its statutory damages provision is not punitive). The statute makes Congress’s legislative judgment clear: a range of \$100 to \$1000 is necessary to have the desired compensatory and deterrent effect and to achieve the FCRA’s important goals. 15 U.S.C. § 1681n(a)(1)(A); *see also Bateman*, 623 F.3d at 719.

While both federal and state law enforcement agencies continually work to protect consumers, resources are limited. The *Amici* States necessarily rely on private litigants to supplement their efforts, particularly where, as here, substantial private interests are at stake.⁵⁸ To limit individual litigants' standing would undermine the FCRA's entire private enforcement scheme as well as recent congressional policy with regard to class actions. One of the explicit purposes of the Class Action Fairness Act of 2005 is to "restore the intent of the framers of the United States Constitution by providing for Federal court consideration of interstate cases of national importance under diversity jurisdiction[.]" Pub. L. No. 109-2, 119 Stat. 4, § 2(b)(2). Yet, consumers barred from bringing federal actions on standing grounds will be limited to seeking redress (individually or collectively) in state court.

Additionally, the availability of private enforcement through class litigation serves as an important deterrent to statutory violations where individual damages are small or hard to separately quantify, as

⁵⁸ See, e.g., *Holman v. Experian Info. Solutions, Inc. et al*, C.A. No. 11-00180, Dkt. No. 279, at pp. 4-5 & 7 (N.D. Cal. Dec. 29, 2014) (approving a class action settlement following Experian's willful violation of the FCRA by selling plaintiffs' credit information to a debt collector for impermissible purposes and finding the settlement amount of \$375 to each class member who submitted a valid claim (1,317 of approximately 38,000 class members) "well within the range of potential statutory damages" provided by the FCRA, and that the payment of \$2,250,000 in costs and attorneys' fees was also reasonable to ensure that the congressional policy embedded in the FCRA – "to redress[] [important] public interest claims" – "will be vindicated").

they often are in the FCRA context. *See Murray*, 434 F.3d at 953 (“Rule 23(b)(3) was designed for situations such as [the FCRA], in which the potential recovery is too slight to support individual suits, but injury is substantial in the aggregate.”). That large financial awards are possible does not mean that class litigation is being abused.⁵⁹ “[S]ociety may gain from the deterrent effect of financial awards” of class litigation, which will prompt consumer reporting agencies to be appropriately cautious with sensitive personal data and to ensure its accuracy and security. *Murray*, 434 F.3d at 953. Even if the FCRA creates incentives for some aggressive plaintiffs or “testers” – who have long been “praised rather than vilified” in the housing and employment contexts – such collective actions vindicate important private rights and, ultimately, help correct abusive practices. *Id.* at 954.

⁵⁹ Contrary to the impression created by Petitioner’s and its *amici*’s invocation of potential uncontrolled class action abuse, the State Attorneys General, who are required to receive notice of all class action settlements (*see* 28 U.S.C. §§ 1715(b), (d)), actively monitor and evaluate them for abuse. *See, e.g., Figueroa v. Sharper Image Corp.*, 517 F. Supp. 2d 1292, 1328 (S.D. Fla. 2007) (stating that the “appearance of the Attorneys General of thirty-five states and the District of Columbia, representing hundreds of thousands, if not millions, of eligible class members,” who “objected at every turn to each version of the parties’ proposed coupon settlement” with “vigor and substance,” “counsels against a finding favorable to the parties”); *Wilson v. DirectBuy, Inc.*, No. 3:09-CV-590JCH, 2011 WL 2050537, at *9 (D. Conn. May 16, 2011) (noting the brief of thirty-nine attorneys general “forcefully argu[ing] that the settlement is both overstated and undervalued” was “especially helpful and ... a placeholder for many absent class members’ objections”).

CONCLUSION

For the foregoing reasons, the Court should affirm the judgment of the court of appeals.

Respectfully submitted,

MAURA HEALEY

Attorney General of Massachusetts

SARA CABLE*

FRANCESCA L. MICELI

Assistant Attorneys General

Office of the Attorney General

One Ashburton Place

Boston, MA 02108

(617) 727-2200

sara.cable@state.ma.us

** Counsel of Record for Amici Curiae*

Dated: September 8, 2015