IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

DR. JAMES ALBERT MCALEER & LINDA MCALEER, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

DEEP ROOT ANALYTICS, LLC, a Virginia limited liability company,

Defendant.

Case No.: 6:17-CV-1142-ORL-18-TBS

CLASS ACTION COMPLAINT, REQUEST FOR INJUNCTIVE RELIEF, AND DEMAND FOR JURY TRIAL

Plaintiffs brings this Class Action Complaint against Deep Root Analytics ("Deep Root"), a Virginia limited liability company, on behalf of themselves and all others similarly situated, and allege, upon personal knowledge and their counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF ACTION

1. Plaintiffs bring this class action against Deep Root for failing to secure and safeguard the public's personally identifiable information ("PII") such as names, addresses, email addresses, telephone numbers, dates of birth, reddit.com browsing history, and voter ID number, which Deep Root collected from many sources, including the Republican National Committee ("RNC") (collectively, "Private Information"), and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class members that their Private Information had been stolen and was and is still vulnerable; and for failing to provide timely, accurate and adequate notice of precisely what specific types of Private Information were stolen.

2. This is not a case in which nefarious hackers "breached the mainframe" and stole sensitive information. This is a case in which Deep Root, the custodian of the Private Information of *nearly 200 million Americans* put that Private Information online without a password.

JURISDICTION AND VENUE

3. This Court has jurisdiction under 28 U.S.C. § 1332, for diversity jurisdiction. The amount in controversy exceeds $5,000,000, and at least two Class Plaintiffs—namely, Dr. James Albert McAleer and Linda McAleer (the "McAleers")—are citizens of Florida, while Deep Root is a citizen of Virginia.

4. This Court has personal jurisdiction over Deep Root because it collected data from Florida residents. In particular, according to the initial report on the breach, the database contained information for the 2016 election only for Florida and Ohio.

5. Venue is proper in the Middle District of Florida because the harm described below occurred in this jurisdiction.

PARTIES

6. Plaintiffs, the McAleers, are Florida citizens, currently living at 264 Spring Run Circle, Longwood, Florida 32779. Their data was stolen from Deep Root.

7. Class Plaintiffs are defined *infra*.

8. Deep Root is a Virginia limited liability company, duly organized under the laws of Virginia, with its principal place of business at 1600 Wilson Blvd., Suite 330, Arlington, Virginia 22209.

FACTUAL BACKGROUND

9. To win in politics, it is vital to understand the target constituency. Today, it is easier than ever to do so due to the sheer amount of information citizens knowingly and unknowingly disseminate about themselves to the Internet.

10. Therefore, in anticipation of the 2016 U.S. election cycle, the RNC employed Deep Root as a data analytics contractor.

11. In this capacity, Deep Root collected the sensitive Private Information of over 198 million U.S. citizens to analyze a voter's proclivities, such as where the voter might fall on issues like gun ownership and abortion.

12. Though Deep Root has only existed since 2013, it had access to information the RNC's other data analytics contractors had collected for the 2008 and 2012 elections.

13. Despite the sensitivity of the information it curated, Deep Root stored the Private Information on a cloud server, as discovered by UpGuard cyber risk analyst Chris Vickey (the "UpGuard Report"). *See* Dan O'Sullivan, *The RNC Files: Inside the Largest US Voter Data Leak*, UPGUARD (June 19, 2017), https://www.upguard.com/breaches/the-rnc-files, attached to this Complaint as Exhibit A.

14. The Private Information was not even password protected.

15. Therefore, during early June, anyone in the world could take the Private Information. It is unknown at this time how many breaches occurred. (Collectively, the "Data Breach").

16. The Data Breach is the largest leak of U.S. voter data in history. *See* Ex. A.

17. Deep Root's goal in collecting the Private Information in the first place was to assemble a complete political profile of nearly every American voter. As such, the Private

Information includes not only raw data, but also includes personal information about each American's beliefs. *See* Ex. A.

18. Since the Data Breach, Deep Root has taken "full responsibility" for it and has only now decided to "update the access settings and put protocols in place to prevent further access." *See* Deli Cameron & Kate Conger, *GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters*, GIZMODO (June 19, 2017, 8:00 AM), http://gizmodo.com/gop-data-firm-accidentally-leaks-personal-details-of-ne-1796211612.

19. Despite this information being publicly available, without password protection, for an indeterminate amount of time, Deep Root only publicly commented on it after the release of the UpGuard Report.

20. The President of the United States is on record as denouncing these sorts of breaches as "gross negligence": "*Gross negligence* by the Democratic National Committee allowed hacking to take place. The Republican National Committee had a strong defense!" Donald J. Trump (@realDonaldTrump) (Jan. 6, 2017, 7:53 PM), https://twitter.com/realDonaldTrump/status/817579925771341825. Apparently, they did not.

Class Action Allegations

21. **Class definitions.** Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a Nationwide class and a Florida class. The **Nationwide class** is initially defined as follows: All persons residing in the United States whose Private Information was disclosed in the Data Breach affecting Deep Root in 2017 (the "Nationwide Class"). The **Florida class** is defined as all persons residing in Florida whose

Private Information was disclosed in the Data Breach affecting Deep Root in 2017 (the "Florida Class").

22. **Class exclusions.** Excluded from each of the above Classes are Deep Root, including any entity in which Deep Root has a controlling interest, is a parent or subsidiary, or which is controlled by Deep Root, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Deep Root. Also excluded are the judges and court personnel in this case and any members of their immediate families.

23. **Numerosity.** Pursuant to Fed. R. Civ. P. 23(a)(1), the members of each Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the UpGuard Report suggests it is over 198 million—roughly 86.5% of the U.S. population over the age of 18.

24. **Commonality.** Pursuant to Fed. R. Civ. P. 23(a)(2) and (b)(3), there are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. How many documented breaches actually occurred;

b. The type of information available from the cloud server;

c. Whether Deep Root failed to implement reasonable security procedures and practices;

d. Whether Deep Root negligently mishandled the data of over 198 million voters by, among other things, storing the Private Information on a cloud server without password protection;

e. Which security procedures and which data-breach notification procedure should Deep Root be required to implement as part of any injunctive relief ordered by the Court;

f. As to the Florida class, whether Deep Root violated Florida's privacy laws in connections with the actions described herein;

g. Whether Deep Root acted negligently in delaying or failing to inform Plaintiffs and the Class Members of the Data Breach;

h. Whether Deep Root's conduct was unfair, deceptive, or unconscionable;

i. What the nature of the relief should be, including equitable relief, to which Plaintiffs and the Class Members are entitled.

j. Whether Plaintiffs and the Class Members have sustained monetary loss and the proper measure of that loss; and

k. Whether Plaintiff and the Class Members have sustained consequential loss and, if so, to what measure.

25. **Ascertainability.** All members of the proposed classes are readily ascertainable. Deep Root has a copy of the Private Information for all members of both classes.

26. **Typicality.** Pursuant to Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members because Plaintiffs' Private Information, like that of every other class member, was misused or disclosed through Deep Root's negligent handling of it.

27. **Adequacy of Representation.** Pursuant to Fed. R. Civ. P. 23(a)(4), Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigation class actions, including privacy litigation.

28. **Superiority of Class Action.** Pursuant to Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Further, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

29. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Deep Root's violations of law inflicting substantial damages in the aggregate would go un-remedied.

30. Class certification is also appropriate under Fed. R. Civ. P. 23(a)) and (b)(2) because Deep Root has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

COUNT I: Negligence
(on behalf of Plaintiffs and the Nationwide Class)

31. Plaintiffs incorporate and re-allege paragraphs 1–30.

32. Upon accepting and storing Plaintiffs and Class Members' Private Information in their respective computer database systems, Deep Root undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Deep Root knew that the Private Information was private and confidential and would be protected accordingly.

33. The law imposed an affirmative duty on Deep Root to timely discover and disclose the unauthorized access and theft of the Private Information to Plaintiffs and the Class

so that Plaintiffs and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

34. At the very least, the law imposed an affirmative duty for Deep Root to, at a minimal level of protection, *put a password* on such sensitive Private Information.

35. Deep Root breached its duty to discover and to notify Plaintiffs and Class Members of the unauthorized access and public availability of the Private Information to Plaintiffs and the Class Members until the third-party UpGuard Report uncovered the public availability of the cloud server. To date, Deep Root has not provided sufficient information to Plaintiffs and the Class Members regarding the extent of unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

36. Deep Root also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles (such as password protection), despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Deep Root failed to provide adequate supervision and oversight of the Private Information in its collection, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

37. Through Deep Root's acts and omissions described in this Complaint, including Deep Root's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Deep Root unlawfully breached its duty to use reasonable care to adequately

protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Deep Root's possession or control.

38. Further, through its failure to timely discover and provide clear notification of the Data Breach to consumers, Deep Root prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information.

39. Upon information and belief, Deep Root improperly and inadequately safeguarded the Private Information of Plaintiff and Class Members in deviation from standard industry rules, regulation, and practices at the time of the Data Breach.

40. Deep Root's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive Private Information, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

41. Deep Root's conduct was grossly negligent (*see* Trump, *supra*) and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' Private Information; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

42. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information.

43. At least one third party has accessed the Private Information stored on Deep Root's cloud server.

44. As a direct and proximate cause of Deep Root's conduct, Plaintiffs and the Class Members suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching adverse and detrimental consequences of identity theft and loss of privacy.

45. To whatever extent that no actual identity theft has yet occurred to Plaintiffs or a given Class Member, the disclosure of the Private Information creates an objectively reasonable likelihood that such an injury will occur. Deep Root's negligence in handling the Private Information has caused an increased risk of future harm to Plaintiffs and the Class Members, as well as a loss of privacy.

WHEREFORE, Plaintiffs, individually and on behalf of all members of the Nationwide class, respectfully request this Court render an order granting Plaintiffs and the Class:

A. actual damages in the amount to be determined at trial, but considerably more than $5,000,000, to compensate them for the loss caused by the wrongful disclosure of their Private Information and Deep Root's failure to notify or to protect the Private Information;

B. injunctive relief requiring Deep Root to secure the Private Information in accordance with contemporary cybersecurity standards;

C. exemplary and punitive damages; and

D. Plaintiffs' reasonable attorneys' fees.

COUNT II: Negligence Per Se
(on behalf of Plaintiffs and the Florida class)

46. Plaintiffs incorporate and re-allege paragraphs 1–45.

47. Deep Root is a covered entity within the meaning of the Florida Information Protection Act of 2013 (FIPA), Fla. Stat. § 501.171, because it acquires, maintains, stores, and

uses personal information, including, but not limited to, the Private Information and the voter ID numbers contained therein. *See* Sullivan, *supra* ¶ 13 (including StateVoterID as a parameter assigned to each potential voter).

48. FIPA requires covered entities to "take reasonable measures to protect and secure data in electronic form containing personal information" and to timely notify any individual whose personal information was stolen as a result of a data breach.

49. Deep Root's failure to timely notify Plaintiffs and the Florida class that their Private Information was available online violated FIPA. To date, Deep Root has not sent Plaintiffs the notice required by Fla. Stat. § 501.171(4)(d).

50. Deep Root's failure to adequately safeguard Plaintiffs and the Florida class's data, even by password protecting it, violated FIPA.

51. As a direct and proximate cause of Deep Root's conduct, Plaintiffs and the Class Members suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discovery and detect, given the far-reaching adverse and detrimental consequences of identity theft; an increased risk of future harm to Plaintiffs and the Class Members; and loss of privacy.

52. To whatever extent that no actual identity theft has yet occurred to Plaintiffs or a given Class Member, the disclosure of the Private Information creates an objectively reasonable likelihood that such an injury will occur.

WHEREFORE, Plaintiffs, individually and on behalf of all members of the Florida class, respectfully request this Court render an order granting Plaintiffs and the Class:

A. actual damages in the amount to be determined at trial, but considerably more than $5,000,000, to compensate them for the loss caused by the wrongful

disclosure of their Private Information and Deep Root's failure to notify or to protect the Private Information;

B. injunctive relief requiring Deep Root to secure the Private Information in accordance with contemporary cybersecurity standards;

C. exemplary and punitive damages; and

D. Plaintiffs' reasonable attorneys' fees.

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted this 20th day of June, 2017.

/s/ David S. Oliver Trace Jackson Attn. of record
David S. Oliver
Florida Bar No. 521922
Primary Email Address:
david.oliver@gray-robinson.com
Secondary Email Address:
donna.flynn@gray-robinson.com
Jason A. Zimmerman
Florida Bar No. 104392
Primary Email Address:
jason.zimmerman@gray-robinson.com
Secondary Email Address:
christine.persampiere@gray-robinson.com
Trace H. Jackson
Florida Bar No. 125693
Primary Email Address:
trace.jackson@gray-robinson.com
GrayRobinson, P.A.
301 East Pine Street, Suite 1400 (32801)
P.O. Box 3068
Orlando, Florida 32802
Telephone: (407) 843-8880
Facsimile: (407) 244-5690

Exhibit A

The RNC Files: Inside the Largest US Voter Data Leak

Updated on June 19, 2017 by Dan O'Sullivan

Filed under: data breaches (https://www.upguard.com/breaches/topic/data-breaches)

In what is the largest known data exposure of its kind, UpGuard's Cyber Risk Team can now confirm that a misconfigured database containing the sensitive personal details of over 198 million American voters was left exposed to the internet by a firm working on behalf of the Republican National Committee (RNC) in their efforts to elect Donald Trump. The data, which was stored in a publicly accessible cloud server owned by Republican data firm Deep Root Analytics (https://app.upguard.com/webscan?url=https://www.deeprootanalytics.com/), included 1.1 terabytes of entirely unsecured personal information compiled by DRA and at least two other Republican contractors, TargetPoint Consulting, Inc. (https://app.upguard.com/webscan?url=https%3A%2F%2Fwww.targetpointconsulting.com%2F) and Data Trust (https://app.upguard.com/webscan?url=http://thedatatrust.com/). In total, the personal information of potentially near all of America's 200 million registered voters (http://www.politico.com/story/2016/10/how-many-registered-voters-are-in-america-2016-229993) was exposed, including names, dates of birth, home addresses, phone numbers, and voter registration details, as well as data described as "modeled" voter ethnicities and religions.

This disclosure dwarfs previous breaches of electoral data in Mexico (https://www.dailydot.com/layer8/amazon-mexican-voting-records/) (also discovered by Vickery) and the Philippines (http://www.wired.co.uk/article/philippines-data-breach-fingerprint-data) by well over 100 million more affected individuals, exposing the personal information of over sixty-one percent of the entire US population.

The data exposure provides insight into the inner workings of the Republican National Committee's $100 million data operation for the 2016 presidential election, an undertaking of monumental scope and painstaking detail (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/) launched in the wake of Mitt Romney's loss in 2012. Deep Root Analytics, TargetPoint, and Data Trust—all Republican data firms—were among the RNC-hired outfits working as the core of the Trump campaign's 2016 general election data team (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/), relied upon in the GOP effort to influence potential voters and accurately predict their behavior. The RNC data repository would ultimately acquire roughly 9.5 billion data points regarding three out of every five Americans, scoring 198 million potential US voters on their likely political preferences using advanced algorithmic modeling across forty-eight different categories.

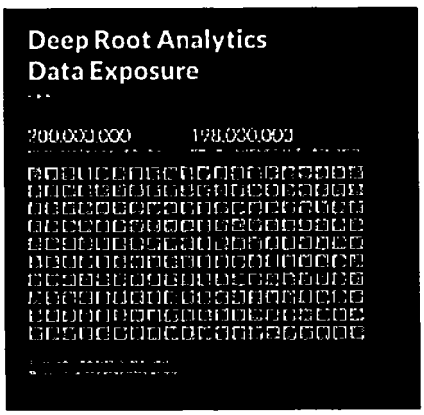
Spreadsheets containing this accumulated data—last updated around the January 2017 presidential inauguration—constitute a treasure trove of political data and modeled preferences used by the Trump campaign. This data was also exposed in the misconfigured database and had been for an unknown period of time.

UpGuard's discovery — of perhaps the largest known exposure of voter information in history—is corroborated by technical evidence, as well as by the public statements of the responsible firms and political staffers.

The Discovery

In the early evening of June 12th, UpGuard Cyber Risk Analyst Chris Vickery discovered an open cloud repository while searching for misconfigured data sources on behalf of the Cyber Risk Team, a research unit of UpGuard devoted to finding, securing, and raising public awareness of such exposures. The data repository, an Amazon Web Services S3 bucket (https://www.upguard.com/solutions/s3-buckets-

configuration-discovery), lacked any protection against access. As such, anyone with an internet connection could have accessed the Republican data operation used to power Donald Trump's presidential victory, simply by navigating to a six-character Amazon subdomain: "dra-dw".



(//www.upguard.com/hubfs/blog-files/breaches/voters-diagram.png?t=1497907768354)Upon inspection of the contents, "dra-dw" is shown to stand for "Deep Root Analytics Data Warehouse." The concept of a "data warehouse" is common in modern business— essentially, it is a massive collection of data prepared specifically for complex analysis. Deep Root Analytics confirmed they owned and operated the dra-dw bucket, which was subsequently secured against public access the night of June 14th, shortly after Vickery notified federal authorities.

In total, 1.1 terabytes of data in the warehouse—an amount roughly equivalent to 500 hours worth of video (https://aimblog.uoregon.edu/2014/07/08/a-terabyte-of-storage-space-how-much-is-too-much/#.WUYMexgrK00)—was fully downloadable. Among these files were clear indications of the repository's political importance, with file directories named for a number of high-powered and influential Republican political organizations. As such, the exposed Deep Root Analytics warehouse contained a remarkable amount of fully accessible data.

Yet this was not all. An additional 24 terabytes of data was stored in the warehouse, but had been configured to prevent public access. Ultimately, the amount of data stored in the misconfigured database was equivalent in size to about 10 billion pages of text.

Less clear was the significance of intriguing but inaccessible files, such as one titled "for_strategy_xroads_updated_FINAL" - which may refer in some capacity to American Crossroads, the Super PAC co-founded by former George W. Bush adviser Karl Rove that was very active in 2016 electoral financing (https://www.opensecrets.org/outsidespending/detail.php?cmte=C00487363). Also found was a large cache of Reddit posts, saved as text:

(https://cdn2.hubspot.net/hubfs/228391/blog-files/breaches/redditcontent.png?t=1497907768354)

It would ultimately take days, from June 12th to June 14th, for Vickery to download 1.1 TB of publicly accessible files, which included two critical directories titled "data_trust" and "target_point."

The Operation

Deep Root Analytics, the Republican data firm which created and maintained the exposed data warehouse, was co-founded in 2013 by Alex Lundry, a Republican campaign data scientist who had served as data director in Mitt Romney's unsuccessful 2012 presidential campaign. The company bills itself (https://www.deeprootanalytics.com/overview/) as "the most experienced group of targeters in Republican politics," offering media analytics services to corporations, lobbying groups, and GOP political campaigns seeking to reach specific target demographics. Deep Root claims to be able to more effectively reach these desired demographics by "microtargeting" using big data analytics, allowing clients to make better-informed decisions when purchasing advertising.

It was a pedigree that would earn Lundry a position as "Chief Analytics Officer" with the 2016 Republican presidential campaign of former Florida Governor Jeb Bush. While Bush would fail to win the nomination even after assembling a well-credentialed data team, Trump would have the inverse problem, winning the nomination without having created a robust data operation within his campaign. Following the formal conclusion of GOP primary season in July 2016 with Trump's nomination, the RNC would move quickly in coordinating their data team's efforts with those of the Trump campaign in the upcoming general election fight against Hillary Clinton (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/).

In order to win the election, the RNC would need to draw heavily upon the resources of several private firms specializing in data analytics. Among these private consultancies was Data Trust (http://thedatatrust.com/), a Washington-based firm that claims to "continually develop a Republican and conservative data ecosystem through voter file collection, development, and enhancement."

Data Trust, "the GOP's exclusive data provider (http://adage.com/article/campaign-trail/rnc-voter-data-provider-joins-ad-firms-including-facebook/303534/)," was created by the RNC in 2011, per *National Review* (http://www.nationalreview.com/article/368581/gops-data-surge-eliana-johnson), "to shoulder the cost of building and managing the

GOP's voter file"—its repository of detailed voter information crucial to any successful electoral advertising and get-out-the-vote efforts. As reported by *Slate* (http://www.slate.com/articles/news_and_politics/victory_lab/2012/01/the_co_op_and_the_data_trust_the_dnc_and_rnc_get_into_the_data Data Trust operates as a private-sector satellite of the RNC—"a hybrid, a private company that party bosses built but can't formally run."

Within the Deep Root Analytics database, the folder "data_trust" appears to contain nothing less than the full fruits of this RNC/Data Trust effort to house as comprehensive and detailed a repository of potential 2016 voter information.

Within "data_trust" are two massive stores of personal information collectively representing up to 198 million potential voters. Consisting primarily of two file repositories, a 256 GB folder for the 2008 presidential election and a 233 GB folder for 2012, each containing fifty-one files - one for every state, as well as the District of Columbia. Each file, formatted as a comma separated value (.csv), lists an internal, 32-character alphanumeric "RNC ID"—such as, for example, 530C2598-6EF4-4A56-9A7X-2FCA466FX2E2—used to uniquely identify every potential voter in the database. These RNC IDS uniquely link disparate data sets together, combining dozens of sensitive and personally identifying data points, making it possible to piece together a striking amount of detail on individual Americans specified by name.

Both Vickery and this reporter looked themselves up in these spreadsheets, confirming that the files contained accurate and sensitive personal information. Listed here are the .csv categories:

"RNCID", "RNC_RegID", "State", "SOURCEID", "Juriscode", "Jurisname", "CountyFIPS", "MCD", "CNTY", "Town", "Ward", "Precinct", "Ballotbox", "PrecinctName", "CD_Current", "CD_NextElection", "SD_Current", "SDProper_Current", "SD_NextElection", "SDProper_NextElection", "LD_Current", "LDS_Current", "LDProper_Current", "LD_NextElection", "LDS_NextElection", "LDProper_NextElection", "NamePrefix", "FirstName", "MiddleName", "LastName", "NameSuffix", "Sex", "BirthYear", "BirthMonth", "BirthDay", "OfficialParty", "StateCalcParty", "RNCCalcParty", "StateVoterID", "JurisdictionVoterID", "AffidavitID", "LegacyID", "LastActiveDate", "RegistrationDate", "VoterStatus", "PermAbs", "SelfReportedDemographic", "ModeledEthnicity", "ModeledReligion", "ModeledEthnicGroup", "HHSEQ", "HTSEQ", "RegistrationAddr1", "RegistrationAddr2", "RegHouseNum", "RegHouseSfx", "RegStPrefix", "RegStName", "RegStType", "RegstPost", "RegUnitType", "RegUnitNumber", "RegCity", "RegSta", "RegZip5", "RegZip4", "RegLatitude", "RegLongitude", "RegGeocodeLevel", "RADR_LastCleanse", "RADR_LastGeoCode", "RADR_LastCOA", "ChangeOfAddress", "COADate", "COAType", "MailingAddr1", "MailingAddr2", "MailHouseNum", "MailHouseSfx", "MailStPrefix", "MailStName", "MailStType", "MailStPost", "MailUnitType", "MailUnitNumber", "MailCity", "MailSta", "MailZip5", "MailZip4", "MailSortCodeRoute", "MailDeliveryPt", "MailDeliveryPtChkDigit", "MailLineOfTravel", "MailLineOfTravelOrder", "MailDPVStatus", "MADR_LastCleanse", "MADR_LastCOA", "AreaCode", "TelephoneNUm", "TelSourceCode", "TelMatchLevel", "TelReliability", "FTC_DoNotCall", "PhoneAppendDate", "VH12G", "VH12P", "VH12PP", "VH11G", "VH11P", "VH10G", "VH10P", "VH09G", "VH09P", "VH08G", "VH08P", "VH08PP", "VH07G", "VH07P", "VH06G", "VH06P", "VH05G", "VH05P", "VH04G", "VH04P", "VH04PP", "VH03G", "VH03P", "VH02G", "VH02P", "MT10_Party", "MT10_GenericBallot", "MT10_Turnout", "MT10_ObamaDisapproval", "MT10_Jobs", "MT10_Healthcare", "MT10_SoCo", "PG01", "PG02", "PG03", "PG04", "PG05", "PG06", "PG07", "PG08", "PG09", "PG10", "PG11", "PG12", "PG13", "PG14", "PG15", "PG16", "PG17", "PG18", "PG19", "PG20", "PG21", "PG22", "PG23", "PG24", "PG25", "PG26", "PG27", "PG28", "PG29", "PG30", "PG31", "PG32", "PG33", "PG34", "PG35", "PG36", "PG37", "PG38", "PG39"

Starting with the potential voter's first and last names—limiting even the barest possibility of the data sets masking the identities of those described—the files go onto list a a great deal more data, including the voter's date of birth, home and mailing addresses, phone number, registered party, self-reported racial demographic, voter registration status, and even whether they are on the federal "Do Not Call" list. Also included as data fields are the "modeled ethnicity" and "modeled religion" of the potential voter—particularly sensitive personal details that have historically been a source of controversy for data collection (https://www.brookings.edu/opinions/why-census-is-right-to-ask-for-racial-and-ethnic-data/).

While not every field is populated for each individual, if the answer is known, it appears to have been included. A smaller folder for the 2016 election was also included in the database, but unlike the 2008 and 2012 folders, only included .csv files for Ohio and Florida - arguably the two most crucial battleground states. The entire "data_trust" folder, it bears repeating, was entirely downloadable by any individual accessing the URL of the database.

This exposure of the personal information of millions of Americans was not, perhaps, the most damaging pool of data exposed. To understand its significance, additional context is necessary.

The RNC's multiyear effort in building a world-class data operation would come to employ Deep Root Analytics in a partnership with other data firms to do for the RNC what Obama's data team had done for the Democrats, as reported by *Ad Age* in a detailed post-election profile of the RNC data operation (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-

win/307105/):

> *"In this case, the people doing most of the data modeling and voter scoring – especially for field operations, voter contact and television advertising -- were from a collective of three data firms hired by the RNC: TargetPoint Consulting, Causeway Solutions, and Deep Root Analytics, which officially worked with the RNC through a new subsidiary called Needle Drop."*

RNC payments to two of the firms mentioned in the database totaled over $5 million, as also reported by *Ad Age* (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/):

> *Between January 2015 and November 2016, the RNC paid TargetPoint $4.2 million for data services, and gave Causeway around $500,000 in that time, according to Federal Election Commission reports. Deep Root, acting as Needle Drop, was paid $983,000 by the RNC.*

Needle Drop principal TargetPoint Consulting (https://www.targetpointconsulting.com/products-services/)—where Deep Root Analytics founder Alex Lundry was employed as "Chief Data Scientist" from 2005 to 2015—is referenced in the database with a folder titled "target_point." TargetPoint, a GOP-aligned, Alexandria, Virginia-based "full service market research and knowledge management firm," specializes in microtargeting key demographics on behalf of corporate and political clients—a tactic they claim to have pioneered (https://www.targetpointconsulting.com/ourwork/) "after President George W. Bush deployed our services for his successful 2004 campaign."

TargetPoint is a trusted and well-established authority on data operations within conservative political circles, having worked in the past on Rudy Giuliani's 2008 presidential bid, the 2008 McCain/Palin campaign, and the National Republican Senatorial Committee's reelection efforts. TargetPoint founder Alexander Gage, a former polling and market researcher, explained to the *Washington Post* in 2007 (http://www.washingtonpost.com/wp-dyn/content/article/2007/07/04/AR2007070401423.html) his philosophy of data analytics while serving as presidential candidate Mitt Romney's Director of Strategy:

> *"'Microtargeting is trying to unravel your political DNA,' [Gage] said. 'The more information I have about you, the better.' The more information [Gage] has, the better he can group people into "target clusters" with names such as 'Flag and Family Republicans' or 'Tax and Terrorism Moderates.' Once a person is defined, finding the right message from the campaign becomes fairly simple."*

While it may be better for data firms like TargetPoint to stockpile your most sensitive personal information, for the 198 million Americans whose sensitive identifying details and potential political inclinations were compiled on a public-facing cloud server lacking any security barriers, the view may be different.

The contents of the "target_point" folder were even more intrusive than those of the Data Trust repository, if less obviously intimidating at first glance: fourteen files saved in the Alteryx Database format (.yxdb), a file format designed specifically for large-scale data analysis. Most of the files were last updated in mid to late-January 2017, with several labeled as "Contact File," with different dates signifying when they were updated.

Contained within these "Contact File" spreadsheets are the aforementioned 32-character alphanumeric RNC IDs for 198 million potential American voters, as well as the corresponding names and addresses of the voters. The clear linkage between every RNC ID and the name and identifying personal details of all 198 million people ensures all data using the RNC ID as an identifier can be tied back to the person's real name.

The remaining files provide a rare glimpse into a systematic large-scale analytics operation being performed using a massive repository of 198 million potential voters, combining personal details, backgrounds, and political behavior to, paraphrasing Gage, "unravel their political DNA". The result is a database of grand scope and scale, collecting the modeled personal and political preferences of most of the country—adding up to an unsecured political treasure trove of data which was free to download online.

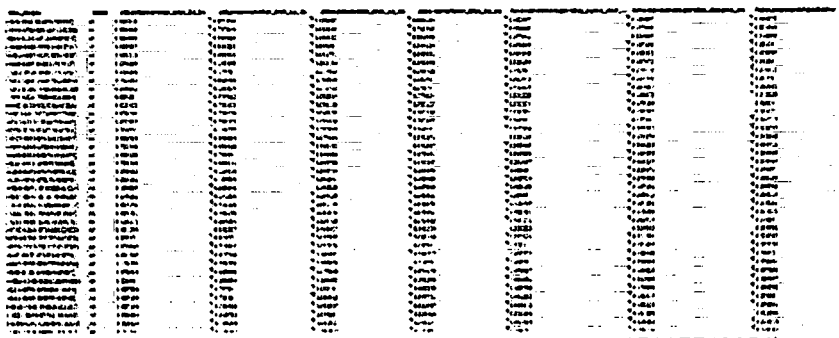
The file dates and names indicate the other files largely concern post-election data analytics conducted in the run-up to and around Trump's inauguration on January 20th, 2017. Some of the files align with public statements by RNC and TargetPoint officials about the kind of targeted analysis performed over the course of the campaign. A file titled "DRA Post Elect 2016 Reluctant DJT scores 1-6-17.yxdb," for example, contains 69 million rows, and is illustrative of the kind of post-election analysis in the repository executed by the

GOP data team. The likelihood of this analysis as a product of the RNC data team is corroborated by public disclosures in the press of similar microtargeting (http://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/), such as TargetPoint's analysis of "'DJT Underperform' voters, or Republicans still unconvinced about supporting Mr. Trump."

In the 50 GB file titled "DRA Post Elect 2016 All Scores 1-12-17.yxdb," each potential voter is scored with a decimal fraction between zero and one across forty-six columns. Each of the fields under each of the forty-six columns signifies the potential voter's modeled likelihood of supporting the policy, political candidate, or belief listed at the top of the column, with zero indicating very unlikely, and one indicating very likely.

RNC_RegID, State, 2012ObamaVoter_DRA_12_16, 2012RomneyVoter_DRA_12_16, 2016ClintonVoter_DRA_12_16, 2016TrumpVoter_DRA_12_16, AmericaFirstForeignPolicy_agree_DRA_12_16 AmericaFirstForeignPolicy_disagree_DRA_12_16 AutoCompaniesShipJobsOverseas_agree_DRA_12_16 AutoCompaniesShipJobsOverseas_disagree_DRA_12_16 CorpReputs_AmericanMakers_DRA_12_16, CorpReputs_DailyLives_DRA_12_16, CorpReputs_Egalitarians_DRA_12_16, CorpReputs_EnviroConscious_DRA_12_16, CorpReputs_OpportunitySeekers_DRA_12_16, CorpReputs_STEMSupporters_DRA_12_16, CorpReputs_SupplyChainers_DRA_12_16, CorpReputs_Unifers_DRA_12_16, DemLeadersStandUpToTrump_DRA_12_16, DemLeadersWorkWithTrump_DRA_12_16, DParty_DRA_12_16, FinancialServicesHarmful_agree_DRA_12_16 FinancialServicesHarmful_disagree_DRA_12_16 FinServicesCompany_Dreamers_DRA_12_16 FinServicesCompany_RiskMitigators_DRA_12_16 FossilFuelsImportantForUSEnergySecurity_DRA_12_16 FossilFuelsNeedToMoveAwayFrom_DRA_12_16, InvestInfrastructure_agree_DRA_12_16, InvestInfrastructure_disagree_DRA_12_16, LowerTaxes_agree_DRA_12_16, LowerTaxes_disagree_DRA_12_16, NonReluctantDJTVoter_DRA_12_16, NonReluctantHRCVoter_DRA_12_16, PharmaCompsDoGreatDamage_agree_DRA_12_16, PharmaCompsDoGreatDamage_disagree_DRA_12_16, ReformGovtRegulations_agree_DRA_12_16, ReformGovtRegulations_disagree_DRA_12_16, ReluctantDJT_Above.5_DRA_12_16, ReluctantHRCVoter_DRA_12_16, RepealObamacare_agree_DRA_12_16, RepealObamacare_disagree_DRA_12_16 RParty_DRA_12_16, StopIllegalImmigration_agree_DRA_12_16, StopIllegalImmigration_disagree_DRA_12_16, TrumpStandUpToDems_DRA_12_16, TrumpWorkWithDems_DRA_12_16, USAFinancialSituation_Optimistic_DRA_12_16, USAFinancialSituation_Pessimistic_DRA_12_16

Calculated for 198 million potential voters, this adds up to a spreadsheet of 9.5 billion modeled probabilities, for questions ranging from how likely it is the individual voted for Obama in 2012, to whether they agree with the Trump foreign policy of "America First," to how likely they are to be concerned with auto manufacturing as an issue, among others.



(https://cdn2.hubspot.net/hubfs/228391/blog-files/breaches/voteprojections.png?t=1497907768354)

The spreadsheet is an impressive deployment of analytical might. However, while each potential voter is signified by their 32-character RNC internal ID, it is a one-step process to determine the real name associated with the modeled policy preferences, as the aforementioned "Contact File" also exposed in the database links the RNC ID to the potential voter's actual identity.

This reporter was able, after determining his RNC ID, to view his modeled policy preferences and political actions as calculated by TargetPoint. It is a testament both to their talents, and to the real danger of this exposure, that the results were astoundingly accurate.

The Significance

This exposure raises significant questions about the privacy and security Americans can expect for their most privileged information. It also comes at a time when the integrity of the US electoral process has been tested by a series of cyber assaults against state voter databases (https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections),

sparking concern that cyber risk could increasingly pose a threat to our most important democratic and governmental institutions.

That such an enormous national database could be created and hosted online, missing even the simplest of protections against the data being publicly accessible, is troubling. The ability to collect such information and store it insecurely further calls into question the responsibilities owed by private corporations and political campaigns to those citizens targeted by increasingly high-powered data analytics operations.

What is beyond debate in 2017 is the increasing inability to trust in the integrity of information technology systems, particularly at scale. As reliance on technology increases, so too grows the cyber risk surface; as more and more functions of life migrate onto digital platforms, more and more functions of life invite cyber risk. Beyond the almost limitless criminal applications of the exposed data for purposes of identity theft, fraud, and resale on the black market, the heft of the data and analytical power of the modeling could be applied to even more ambitious efforts - corporate marketing, spam, advanced political targeting. Any of these potential misuses of private information can be prevented, provided stakeholders obey a few simple precepts in collecting and storing data.

The fundamental problems which exposed this data are not rare, uncommon, or consigned to one side of the partisan divide; indeed, while those responsible for this exposure are of one party, the 198 million Americans affected span the entire political spectrum, their information revealed regardless of their political beliefs. The same factors that have resulted in thousands of previous data breaches—forgotten databases, third-party vendor risks, inappropriate permissions—combined with the RNC campaign operation to create a nearly unprecedented data breach.

Despite the breadth of this breach, it will doubtlessly be topped in the future—to a likely far more damaging effect—if the ethos of cyber resilience across all platforms does not become the common language of all internet-facing systems.

Cyber Risk Researcher
Chris Vickery
Recognized within the community for his prowess in discovering exposed data and misconfigured assets, Chris is a pioneer in the ethical documentation and analysis of this creeping data security epidemic.

UpGuard Journalist
Dan O'Sullivan
Appearing in *Rolling Stone*, *VICE*, *Jacobin*, *Gawker*, *The Daily Beast*, and *Best American Sports Writing 2015*, Dan's work is well-known for his powerful linguistic style and storytelling ability.

Media Relations
Kelly Rethmeyer
Previously working alongside some of technology's most interesting companies, Kelly excels in communicating complex data security issues to a wide audience. She can be reached at kelly.rethmeyer@upguard.com (mailto:kelly.rethmeyer@upguard.com).

JS 44 (Rev. 11/15)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Dr. James Albert McAleer and Linda McAleer, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Seminole
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

David S. Oliver, Jason A. Zimmerman, Trace H. Jackson
GrayRobinson, P.A., 301 E. Pine St., Orlando, FL 32801

DEFENDANTS

Deep Root Analytics, LLC

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. 1332

Brief description of cause:
Negligence in mishandling the data of over 198 million U.S. citizens

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 06/20/2017

SIGNATURE OF ATTORNEY OF RECORD /s/David S. Oliver Trace Jackson Atty. of Record

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____