UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

SCOTT MOORE, JAMES LONG, AND NANCY PERRY, on behalf of themselves and all others similarly situated, *Plaintiffs*,	)	Case No._____
v.	)	
KRIS KOBACH, in his individual capacity and official capacity as the Secretary of State of Kansas, *Defendant*.	)	

CLASS ACTION COMPLAINT

Plaintiffs, on behalf of themselves and all others similarly situated, by and through undersigned counsel, hereby allege as follows:

Introduction

1. This is a case about Kansas Secretary of State Kris Kobach's reckless disclosure of private personal information entrusted to him by thousands of Kansas voters.
2. Plaintiffs bring this action to enjoin Defendant Kobach from continuing to maintain, share, and release their sensitive voter registration information, including their partial social security number, to other states in connection with the Interstate Voter Registration Crosscheck Program (hereinafter "Crosscheck"). Further, Plaintiffs seek to remedy past disclosures of their sensitive personal information exposed as a result of Kansas's participation in Crosscheck. Plaintiffs challenge Defendant Kobach's reckless maintenance

and disclosure of their private voter data as an unconstitutional invasion of privacy and a violation of the Kansas Public Records Act, which prohibits government disclosure of social security numbers.

3. Crosscheck is a data comparison program administered by Defendant Kobach and used to compare voter registration information among participating states, including Kansas. The program is free of charge to participating states and is exclusively funded by Kansas taxpayers.[1] Crosscheck compares registration lists and analyzes voters' first name, surname, and date of birth to determine whether individuals are registered in multiple states. Because the matching criteria yields false positive results in 99.5% of cases,[2] Defendant Kobach encourages states to provide voters' partial social security numbers and other confidential information to narrow the list of possible double registrants.

4. As the operator of Crosscheck, Defendant Kobach and his staff are responsible for comparing voter registration lists submitted by participant states and sharing "potential match" result lists with each state. Defendant Kobach is also responsible for coordinating access to the file transfer protocol (hereinafter "FTP") server. As the server administrator, Defendant Kobach regularly emails the FTP server URL and password in plain text emails to dozens of recipients. The server URL and passwords are widely shared and emails containing the password regularly copy non-government officials.[3]

---

[1] Keith Esau, Rep., Presentation at the National Conference of State Legislators: Interstate Voter Registration Crosscheck Program (June 15, 2017), at 7, http://www.ncsl.org/Portals/1/Documents/Elections/Kansas_VR_Crosscheck_Program.pdf.

[2] *See* Sharad Goel, et. al., *One Person, One Vote*: *Estimating the Prevalence of Double Voting in U.S. Presidential Elections* (Oct. 24, 2017) (working paper), https://scholar.harvard.edu/files/morse/files/1p1v.pdf; Sean Gallagher, *Researchers warn state system to catch voter fraud has 99% false positive rate*, Ars Technica (Oct. 31, 2017), https://arstechnica.com/information-technology/2017/10/researchers-warn-state-system-to-catch-voter-fraud-has-99-false-positive-rate/.

[3] *See, e.g.*, Crosscheck Results Encryption Passwords, Endcrosscheck (last visited June 18, 2018), https://www.endcrosscheck.com/foia-security/#resultspasswords.

5. From 2012-2017, the Arkansas Secretary of State's Office hosted the FTP site. However, Defendant Kobach's office assumed responsibility for hosting the site in late 2017 after participating states discovered that Arkansas had failed to fortify the server with even rudimentary security protections.[4]
6. In addition to administering the national Crosscheck program, Defendant Kobach is also responsible for managing Kansas's participation in Crosscheck. Accordingly, Defendant Kobach uploads the voter registration information of 1.3 million Kansans to Crosscheck's FTP server and shares with other states the sensitive personal information of the more than 150,000 Kansas voters identified as possible double registrants.
7. In order to determine whether Kansans identified as possible double registrants are voting in other states, Defendant Kobach maintains a practice of sharing Kansas voters' partial social security number and other personally identifiable information through unsecure methods, including as unencrypted email attachments.
8. Further, in order to identify possible double voters, Defendant Kobach sends voters' signatures to other states participating in Crosscheck. Defendant Kobach maintains a practice of sending signatures as an unencrypted email attachment.
9. Since Defendant Kobach began operating Crosscheck in 2011, eight states--including Florida, Alaska, Kentucky, Washington, Oregon, New York, Pennsylvania, and Massachusetts--have left the program due to security risks and data reliability concerns.[5] Kentucky stopped sharing voter data in 2017, citing concerns about Defendant Kobach's

[4] Allison Kite, *Kobach's office will delay data uploads for Crosscheck voter system to accommodate security review*, The Topeka Capital-Journal (Jan. 17, 2018), http://www.cjonline.com/news/20180117/kobachs-office-will-delay-data-uploads-for-crosscheck-voter-system-to-accommodate-security-review.
[5] Dell Cameron, *Eighth state quietly quite crosscheck over security concerns and 'unreliable' results*, Gizmodo (Jan. 29, 2018), https://gizmodo.com/eighth-state-quietly-quit-free-anti-voter-fraud-program-1822514538.

handling of private voter information.[6] Similarly, New York ended its participation in the program in 2016 because "there was no guarantee [Social Security numbers] would be private and majority of records were inaccurate."[7] Other states have indefinitely suspended participation in Crosscheck until Defendant Kobach provides an improved security plan, including Idaho and Illinois. Republican Secretary of State Lawrence Denney explained Idaho's decision to pause participation in Crosscheck stating, "I thought the process was very secure. I had no idea maybe it wasn't. I would just say that it has been very sloppy."[8] In a January 15, 2018 letter to state lawmakers, Illinois State Board of Elections Director Steve Sandvoss stated "we will transmit no data to Crosscheck until security issues are addressed to our satisfaction."[9]

10. Kansas attempted to address concerns about the security of the server in or around October 2017 by assuming responsibility for hosting the site. In January 2018, security firm, Netragard performed an audit of Crosscheck's server security and found the system still lacked industry standard security features and remained vulnerable to hacking.[10] Because Defendant Kobach's office maintained a practice of emailing the server URL and

[6] Alison Grimes (@AlisonForKY), Twitter (Jan. 25, 2018, 4:34 PM), https://twitter.com/AlisonForKY/status/956686808477261824.
[7] *See* Illinois Survey Results, Inter-State Cross Check and ERIC Participation: Individual Responses, https://www.surveymonkey.com/results/SM-FCJWLBZ5/.
[8] Cynthia Sewell, *Idaho will revisit being part of 'sloppy' voter fraud program, says secretary of state*, Idaho Statesman (Nov. 14, 2017), http://www.idahostatesman.com/news/politics-government/state-politics/article184565498.html.
[9] *See Illinois Delays Sending Voter Data to Multi-State Program*, NBC Chicago 5 (Jan. 16, 2018), https://www.nbcchicago.com/news/local/illinois-delays-sending-voter-data-to-multi-state-program-469583963.html.
[10] Dell Cameron, *As Crosscheck Moves to Secure Voter Data, Hacking Fears Grow Among Experts and Politician*, Gizmodo (Jan. 24, 2018), https://gizmodo.com/as-crosscheck-moves-to-secure-voter-data-hacking-fears-1822344007.

encryption passwords in plain text, the audit revealed that any reader of the emails would easily be able to access and download voter records.[11]

11. As the operator of Crosscheck, Defendant Kobach also failed to create and observe practices that would prevent the disclosure of private personal information shared between states as part of the program. In an October 23, 2013 email to Defendant Kobach's office, Florida's Director of Elections Maria Matthews expressed a concern that voter "SSNs may not be protected in other states in a public release."[12] Defendant Kobach's office replied that "hopefully" other states would deny open records request for Crosscheck documents containing voter SSN and conceded the office "would like to find firmer legal footing for denying these requests."[13]

12. As the official responsible for administering Kansas's participation in Crosscheck, Defendant Kobach maintained a practice of sharing the sensitive personal information of Kansas voters with states that may have been required to release the information under their open records laws.[14] At least three states that have participated in Crosscheck lack laws prohibiting the disclosure of social security numbers and other sensitive personal information that Defendant Kobach shares in order to identify potential double registrants.[15]

13. Irrespective of state open records laws, Defendant Kobach's practice of emailing private voter information as an unencrypted attachment creates a substantial risk of inadvertent

---

[11] *Id.*
[12] Email from Maria Matthews, Florida Director of the Division of Elections, to Brad Bryant, former Kansas Director of Elections (Oct. 23, 2013, 8:58 PM).
[13] Email from Brad Bryant, former Kansas Director of Elections, to Maria Matthews, Florida Director of the Division of Elections (Oct. 29, 2013, 2:51 PM).
[14] *Id.*
[15] Idaho Code Ann. § 74-106 (2018); Iowa Code § 22.7 *et seq.*; S.C. Code Ann. § 30-3-310 (2017); S.C. Code Ann. § 30-3-310 (2017).

public disclosure. A risk that materialized in November 2017 when Florida, a state that restricts disclosure of sensitive personal information, inadvertently released the partial social security number and personal identifying information of Kansas voters because Defendant Kobach failed to encrypt a "potential double registrant" list.

14. In November 2017, the Florida Department of State Division of Elections (hereinafter "FDE") released the name, date of birth, address, and partial social security number of 945 Kansas voters, including that of the Plaintiffs.[16] The exposed information was shared by Defendant Kobach's office as an unencrypted attachment to an email sent to FDE.

15. On information and belief, Defendant Kobach continues to maintain protocols and practices that make Kansas voters' private personal information vulnerable to exposure or release. While Defendant Kobach has vaguely committed to making routine upgrades to server security in his capacity as the operator of Crosscheck, he has yet to acknowledge the Kansas Secretary of State's office plans to improve data security practices as a Crosscheck participant, including changes to open records protocols.

16. Defendant Kobach has and continues to recklessly expose private voter data by sending sensitive personal information to participant states that cannot guarantee the confidentiality of these records. Further Defendant Kobach continues to neglect the adoption of adequate security protocols such as encryption transmission practices. Doing so violates voters' constitutional right to privacy and circumvents state public records laws that prohibit the release of social security numbers. Accordingly, Defendants' actions should be enjoined and he should be held liable, in his individual capacity, for violations of state law.

[16] Allison Kite, *Kansas-based Crosscheck spreadsheet compromises 945 voters' data*, The Topeka Capital-Journal (Jan. 19, 2018), http://www.cjonline.com/news/20180119/kansas-based-crosscheck-spreadsheet-compromises-945-voters-data.

Jurisdiction and Venue

17. This action is brought pursuant to 42 U.S.C. §1983.

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1331, as to Plaintiffs' claims under the Fourteenth Amendment of the United States Constitution.

19. This Court has supplemental jurisdiction over this action pursuant to 28 U.S.C. §1367(a), as to Plaintiffs' claims under the Kansas Public Records Act against the Defendant in his individual capacity.

20. This Court has personal jurisdiction over the Defendant because he does business in, and is an elected officer of, the State of Kansas.

21. Venue is proper in this Court pursuant to 28 U.S.C. §1391.

Parties

22. Plaintiff Scott Moore, is a United States citizen and resident of the State of Kansas. He first registered to vote in Douglas County, Kansas when he was 18 years old and attending college at the University of Kansas. Moore re-registered in Johnson County, Kansas in 1998 after he graduated. Since first registering in 1990, Moore has never lived outside of Kansas. Moore's first name, middle name, last name, date of birth, address, and partial social security number were shared as an unsecured email attachment to FDE in January 2013 and released by FDE in response to a November 2017 open records request. Moore is highly concerned that Defendant Kobach's exposure of his sensitive personal information will make him vulnerable to identity theft and further public intrusions into his private financial and personal information. He is also concerned that, due to his common name, Defendant Kobach will continue to identify him as a "potential match" and share his

private information through unsecure methods as part of Kansas's participation in Crosscheck.

23. Plaintiff James Long is a seventy-four year old United States citizen and Navy veteran who resides in Shawnee County, Kansas. He registered to vote in Shawnee County, Kansas in 1961 and has never registered to vote in a jurisdiction outside of the state of Kansas. In January 2013, Defendant Kobach shared Long's first name, middle name, last name, date of birth, address, and partial social security number as an unsecured email attachment to FDE. The attachment was released in response to an open records request in November 2017. Long fears that Defendant Kobach's exposure of his private information has put him at risk for identify theft. Moreover, because Long has a common first and last name, he is concerned that Defendant Kobach will continue to identify him as a possible double registrant and share his private information through unsecure methods.

24. Plaintiff Nancy Perry is a sixty-one year old United States citizen who lives in Shawnee County, Kansas. Perry registered to vote in Kansas in 2005. Since registering, Perry has only lived in Kansas and she has not attempted to register in another state. Perry's first name, middle name, last name, date of birth, address, and partial social security number were exposed in an unsecured email attachment to FDE in January 2013 and released in response to an open records request in November 2017. Perry believes that Defendant Kobach has compromised the security of her personal sensitive information, making her vulnerable to identity theft and other financial harm. She also fears that Kobach will continue to identify her as a "potential match" and share her private information through unsecure methods in the future.

25. Defendant Kris W. Kobach is the Secretary of State of the State of Kansas. He is sued in his individual and official capacities. Defendant Kobach is the State's chief election official responsible for overseeing all election related matters, including voter registration list maintenance, and identifying voters who are possibly registered in another state. In his official capacity as Secretary of State, Defendant Kobach manages Kansas's participation in the Crosscheck program. Further, Defendant Kobach directs Kansas's operation of the Crosscheck program. During his tenure as Secretary of State, Defendant Kobach has been consistently criticized by privacy advocates for his failure to safeguard confidential information entrusted to him by the residents of Kansas. For instance, Defendant Kobach publicly posted the personal information of 106,834 state employees, including his own, in January 2018.[17]

Class Allegations

26. Plaintiffs seek to bring this action on their own behalf and on behalf of a class of those similarly situated pursuant to Rule 23(a) and (b)(2) of the Federal Rules of Civil Procedure.
27. The proposed Class is defined as: "People who (1) are registered to vote in Kansas, and (2) provided their partial social security number on their voter registration form, and (3) had or will have their voter registration information shared with another state or third party through an unsecure method as part of Kansas's participation in Crosscheck."
28. The Class meets all of the requirements of Rule 23(a) of the Federal Rules of Civil Procedure.

[17] Brett Samuels, *Kansas Website exposed state employees' personal information: report*, The Hill (Jan. 25, 2018), http://thehill.com/homenews/state-watch/370743-kansas-website-exposed-state-employees-personal-information-report.

29. The members of the Class are so numerous as to render joinder impracticable. Although the exact size of the class is unknown, nearly 1000 Kansas voters had their information exposed in a single communication in 2013. Defendant's practice of sharing voter's partial social security numbers through email attachments and other unsecure methods occurs on a routine basis and will for the foreseeable future unless such conduct is enjoined by the Court. Moreover, joinder is impracticable because a number of Class members may not know that their rights have been violated.

30. The Class members share a number of questions of law and fact in common, including but not limited to whether Defendant Kobach has and continues to expose private voter data in violation of the Fourteenth Amendment of the United State Constitution and whether voters are entitled to civil penalties under the Kansas Public Records Act.

31. The named Plaintiffs' claims are typical of those of the Class. Like other members of the Class, the named Plaintiffs have been and likely will again be victims of Defendant's reckless disclosures of their voter information in violation of the Fourteenth Amendment.

32. The legal theories under which the named Plaintiffs seek declaratory and injunctive relief are the same or similar to those on which all members of the Class will rely, and the injuries suffered by the Plaintiffs are typical of the injuries suffered by the Class members.

33. The named Plaintiffs: (a) have strong interest in the outcome of this action; (b) have no conflicts of interest with members of the Plaintiff Class, and (c) will fairly and adequately protect the interests of the Class. The Plaintiffs are all individuals who are registered to vote in Kansas. As long as Defendant continues to engage in the conduct described herein, the named Plaintiffs will remain at a substantial risk of suffering constitutional and

statutory violations as a result of Defendant's reckless handling of their private personal information.

34. The named Plaintiffs are represented by the American Civil Liberties Union Foundation of Kansas and Dentons US LLP. Counsel for the Plaintiffs have the resources, expertise, and experience to prosecute this action. Counsel for the Plaintiffs know of no conflicts among members of the Class or between attorneys and members of the Class.

35. The Plaintiff Class should be certified pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure because Defendants have acted on grounds generally applicable to the Class, thereby making Class-wide declaratory and injunctive relief appropriate.

Legal Framework

36. The Fourteenth Amendment right to privacy safeguards against government exposure of personal information in which an individual has a legitimate expectation of confidentiality.

37. This right to informational privacy extends to a range of types of personal information, including "certain financial records, which courts have placed within the ambit of constitutional protection." *Sheets v. Salt Lake County*, 45 F.3d 1383, 1388 (10th Cir. 1995).

38. In particular, individuals have a well-established privacy interest in their social security number. *Int'l Bhd. of Elec. Workers Local Union No. 5 v. U.S. Dep't of Hous. & Urban Dev.*, 852 F.2d 87, 89 (3d Cir. 1988) ("the release of Social Security numbers would constitute a clearly unwarranted invasion of privacy"); *Ostergren v. Cuccinelli*, 615 F.3d 263, 277 (4th Cir. 2010) ("it should not be difficult for a court to conclude that the protection of SSNs from public disclosure should qualify as a State interest of the highest order."); *Greidinger v. Davis*, 988 F.2d 1344, 1354 (4th Cir. 1993) ("the harm that can be

inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous"); *Ferm v. U.S. Tr.* (*In re Crawford*), 194 F.3d 954, 958 (9th Cir. 1999) ("we agree that the indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses may implicate the constitutional right to informational privacy"); *State v. City of Akron*, 640 N.E.2d 164, 168 (Ohio 1994) ("Congress when enacting the Privacy Act of 1974 was codifying the societal perception that SSNs should not be available at all. This legislative scheme is sufficient to create an expectation of privacy."). With advances in technology, a citizen's privacy interest has expanded to his partial social security number. *See, e.g.*, Jonathan J. Darrow & Stephen Lichtenstein, *Do You Really Need My Social Security Number? Data Collection Practices in the Digital Age*, 10 N.C. J.L. & Tech. 1, 47 (2008).

39. Additionally, several courts recognize an individual privacy interest in one's signature. *See Burnett v. County of Bergen*, 968 A.2d 1151 (N.J. 2009) (noting that the combination of SSNs with other personal information, including signatures, "elevates the privacy concern at stake"); *Brannum v. Dominguez*, 377 F. Supp. 2d 75, 84 (D.D.C. 2005) (discussing the individual privacy interest in signatures given their "'personal' [] nature" and the potential that "the release of this information would . . . create opportunity for misappropriation"). The confidential nature of signatures explains the decision of at least twelve states to prohibit the disclosure of voter registration signatures in public records requests.[18]

[18] *See* Alaska Stat. § 15.07.195(a)(6) (2018) ("The following information set out in state voter registration records is confidential and is not open to public inspection: . . . (6) the voter's signature."); Ariz. Rev. Stat. § 16-168(F) (2018) (prohibiting public inspection of "the records containing a voter's signature"); Cal. Elec. Code § 2194(b)(2) (2018) ("[T]he signature of the voter shown on the affidavit of voter registration or an image thereof is confidential and shall not be disclosed to any person"); Colo. Rev. Stat. 24-72-204(8)(a) (2018) (prohibiting the inspection of "the election records of any person that contain the original signature . . . of that person, including electronic, digital, or scanned images of a person's original signature"); Fla. Stat. § 97.0585(2) (2018) ("The signature of a voter registration applicant or a voter is exempt from the copying requirements" of Florida's public records statute);

Releasing personal identifying information in addition to a signature further heightens the risk of identity theft. *See, e.g.*, Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1255 (2003) ("From a speeding ticket placed on [a] website, an identity thief accessed a victim's SSN, address, birth date, *signature*, and other personal information and opened up credit card accounts in the victim's name.") (emphasis added).

40. As the Supreme Court and Tenth Circuit have acknowledged, the collection and maintenance of private information may violate the privacy provisions of the Fourteenth Amendment when the government fails to adopt adequate safeguards that protect against unauthorized disclosure. *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) (holding state collection of drug prescription information did not violate plaintiffs' right to informational privacy because security provisions were sufficient to protect against public disclosure); *Nixon v. Adm'r of Gen. Servs.*¸ 433 U.S. 425, 457 (1977) (holding protections against undue dissemination of private information vitiated Fourteenth Amendment concerns created by collection of private information); *Kerns v. Bader*, 663 F.3d 1173, 1186 (10th Cir. 2011) (noting that plaintiff's constitutional privacy claim hinged on whether "information was sufficiently protected against public disclosure."). Notwithstanding the

---

Kibort v. Westrom, 862 N.E.2d 609 (Ill. App. Ct. 2d Dist. 2007) (interpreting 10 Ill. Comp. Stat. 5/17-20 (2018) and 5/17-22 (2018) to exclude the disclosure of poll signatures from public records law); Me. Rev. Stat. Ann. tit. 21-A, § 22 (2018) ("the voter's signature . . . on the voter registration application and associated records in electronic format are designated as nonpublic records and the registrar shall exclude those items from public inspection"); N.C. Gen. Stat. § 163A-871(a) (2018) ("The signature of the voter, either on the paper application or an electronically captured image of it, may be viewed by the public but may not be copied or traced except by election officials for election administration purposes."); Or. Rev. Stat. § 247.973(2) (2018) ("A person may not make a copy of . . . an individual's signature submitted under this chapter for purposes of registering to vote"); 4 Pa. Code § 183.14(c) (2018) ("The following items may not be made available for public inspection or photography: (1) The signature of a registrant or applicant"); Tenn. Code Ann. § 2-2-127 (2018) (permitting public *inspection* of voter registration applications but otherwise prohibiting their removal from elections offices); Wash. Rev. Code § 29A.08.710 (2018) (listing the information on voter registration applications available for public inspection and copying, and excluding voters' signatures).

existence of statutory or procedural safeguards, collection of information may invade privacy rights where actual disclosures have occurred or plaintiffs identify plausible scenarios under which information will be exposed. *NASA v. Nelson*, 562 U.S. 134, 158-59 (2011).

41. Maintenance and disclosure of information in which citizens have an expectation of privacy "must advance a compelling state interest which, in addition, must be accomplished in the least restrictive means." *See Aid for Women v. Foulston*, 441 F.3d 1101, 1119 (10th Cir. 2006).

42. The government's interest in disseminating social security numbers is rarely sufficiently weighty to trump a citizen's expectation of privacy. *See e.g., City of Akron*, 640 N.E.2d at 169 ("the release of . . . SSNs would provide . . . little useful information"). Where the balance of interests are at equipoise, a less intrusive alternative is commonly available. For instance, in the context of election integrity, the Fourth Circuit explained a state's "interest in preventing voter fraud and voter participation could easily be met without the disclosure of the SSN and the attendant possibility of a serious invasion of privacy that would result from disclosure." *Greidinger*, 988 F.2d at 1354. Courts have also identified that redactions or encryptions of sensitive personal data are a less restrictive alternative to sharing or maintaining private information in unredacted form. *See e.g.*, *Denver Policemen's Protective Ass'n. v. Lichtenstein*, 660 F.2d 434, 436 (10th Cir. 1981); *Alpha Med. Clinic v. Anderson*¸ 128 P.3d 364, 378 (Kan. 2006).

43. Plaintiffs have a strong expectation of confidentiality in their social security number, signature, and other personal information they provide to Defendant as part of their voter

registration. Accordingly, Defendant's reckless maintenance and disclosure through Crosscheck implicates Plaintiffs' informational privacy rights.

Factual Allegations

The Interstate Voter Registration Crosscheck Program

44. Former Kansas Secretary of State Ron Thornburg launched Crosscheck in 2005 to help Kansas and neighboring states compare voter data and detect double registrants.

45. The Kansas Secretary of State's office administers Crosscheck by collecting voter registration information from participant states and cross-referencing lists for potential matches.[19] Kansas then generates reports for each participant state listing potential duplicate records.[20]

46. Crosscheck participants principally share data through a FTP site, which was previously hosted by the Arkansas Secretary of State's office. The site is now hosted by the Kansas Secretary of State's office.

47. Participants share data with Kansas by uploading voter rolls to the FTP site. Specifically, each participant state extracts voter data from their registration rolls and prepares the information in accordance with Crosscheck's data format document. The participant state then encrypts their files using a free encryption program and uploads the data to the FTP site.[21] Defendant Kobach used the AxCrypt software to encrypt files prior to 2017. On

[19] Keith Esau, Rep., Presentation at the National Conference of State Legislators: Interstate Voter Registration Crosscheck Program (June 15, 2017), http://www.ncsl.org/Portals/1/Documents/Elections/Kansas_VR_Crosscheck_Program.pdf.
[20] *Id.*
[21] Interstate Voter Registration Data Crosscheck: 2017 Participation Guide, at 7 (Jan. 2017). For an electronic version of a similar 2014 Participation Guide, see Interstate Voter Registration Data Crosscheck: 2014 Participation Guide, p. 8 (Dec. 2013),

information and belief, he now uses the free encryption program 7-zip. Participants are directed to email the decryption password to Defendant Kobach's office.

48. Participant states are asked to upload their data in January of each year.[22]

49. Once participant states upload their extraction files, Kansas pulls the files from the site, runs a comparison of each state's voter information, and uploads result files to the FTP site.[23] Kansas then notifies each state that their results file is available and emails a decryption passphrase enabling them to open their file. The results file contains a potential match lists, which identifies voters registered in the participant state that share a name and date of birth with a voter in another state.

50. Once states have received their potential match list, they can directly contact the jurisdiction where the voter is potentially double registered. Defendant Kobach advises participant states processing potential match results to obtain a voter's middle name, partial social security number, and signature to determine whether the voter is registered in another state.[24]

51. Each participant state is directed to notify Defendant Kobach about how information requests should be communicated to their office. While the Crosscheck participation guide cautions against sending registrants' personally identifiable information via email, there is no provision restricting unsecure transmissions in the Memorandum of Understanding.[25]

---

https://wei.sos.wa.gov/agency/osos/en/press_and_research/weekly/Documents/Participation%20Guide%20with%20Comments.pdf.

[22] *Id.* at 1.

[23] *Id.*

[24] *Id.* at 3.

[25] *Id.* at 4.

52. Crosscheck uses a two-point match criteria, identifying registered voters that share the same first name, last name, and date of birth.[26] Participant states are also asked to provide additional voter data including partial social security number, voter status, middle name, voter identification number, mailing address, county, date of registration, and whether the voter cast a ballot in the most recent election.[27] In 2017, at least ten states did not provide partial social security numbers for Kansas to narrow results.

53. On information and belief, execution of a memorandum of understanding is the only requirement for states to participate in Crosscheck.

Defendant Kobach's Policies and Practices for Requesting and Transmitting Information

54. As a participant in Crosscheck, Kansas analyzes potential matches by comparing secondary data of voters, including their partial social security number and middle initial. Once Kansas narrows the number of potential matches, it submits information requests to the other state where double voting possibly occurred.

55. Kansas sends the name and date of birth of potential match voters to participant states with a request for documentation of vote history and the voter's signature. On information and belief, Kansas requests states to supply voter signatures as an unencrypted email attachment.[28]

---

[26] Memorandum of Understanding for Interstate Voter Registration Data Comparison, p. 1, ¶ 2(d) (Jan. 2013). For an electronic version of a similar 2012 Memorandum of Understanding, see Memorandum of Understanding for Interstate Voter Registration Data Comparison, p. 1, ¶ 2(d) (Dec. 2012), http://www.girardatlarge.com/wp-content/uploads/2014/06/Ohio-Signed-MOU-2013.pdf.

[27] *Id.* at 4; *see also id.* at 2, ¶ 3.

[28] Email from Jameson Beckner, Kansas Assistant Director of Elections, to Maria Matthews, Florida Director of the Division of Elections (April 29, 2013, 11:56 AM) ("I would also ask that you provide any documentation from the narrowed list that would prove the voters in question did cast a ballot in Florida for the 2012 General Election. Ideally this would be anything with the voter's signature on it. . . . Feel free to reply to this email with any documentation you may be able to provide (a pdf file would be ideal.)"); *see also* FOIA Documents – Open Records Risk, Endcrosscheck (last visited June 18, 2018), https://www.endcrosscheck.com/open-records-risk/.

56. On information and belief, Kansas lacks a method for narrowing potential matches when a state does not provide partial social security numbers or middle initials.

57. Kansas maintains a practice of sending full potential match lists as an unencrypted email attachment to participant states that do not include social security numbers or middle initials in their extraction file. Full match lists include the partial social security number and other personal identifying information of hundreds of voters.[29]

58. According to Kansas Elections Director, Brian Caskey, approximately half the states provide partial social security numbers.[30]

States Begin to Join Crosscheck

59. From 2005 to 2011, Crosscheck had only four participants, Kansas, Iowa, Missouri, and Nebraska. When Defendant Kobach took office in 2011, he pledged to expand Crosscheck, declaring "I have taken it under my wing and want to build it as one of my personal missions."[31]

60. In 2012, ten new states joined Crosscheck, expanding the number of participants to fourteen. By 2016, thirty states were participating in Crosscheck.

61. Over ten years, the Crosscheck program added twenty-six states and 100 million voter records to the comparison database.

---

[29] *Id.* ("We are requesting that Florida examine the attached list of 945 records and narrow the field to only those that still match. . . . This is a bit more complicated than a normal request with another state, but I didn't know of any other way to really examine if any double votes occurred between our two states without middle initial or SSN to narrow the results."); *see also* FOIA Documents – Open Records Risk, Endcrosscheck (last visited June 18, 2018), https://www.endcrosscheck.com/open-records-risk/.

[30] Kansas Secretary of State Security Briefing: Hearing Before the H. Comm. on Govt., Tech. and Security, 87th Leg., 2018 Sess. (Kan. Jan. 22, 2018) (statement of Bryan Caskey, Kansas Elections Director).

[31] Scott Rothschild, *Program run by Kobach checks voter registration records of more than 100 million people*, Lawrence Journal World, (Apr. 20, 2014), http://www2.ljworld.com/news/2014/apr/20/program-run-kobach-checks-voter-registation-record/.

62. Despite this increase in the number of states participating and records compared, Defendant Kobach never developed a more sophisticated protocol for sharing potential matches or ensuring that states maintained voter data shared with them in a secure manner. Additionally, Defendant Kobach downsized his IT staff since the program expanded.[32]

Industry Standard Protocols for Data Maintenance and Transmission

63. Federal and state governments have both recognized the importance of securing the private information of their citizens. The Office of Management and Budget requires federal executive agencies to "[e]ncrypt all . . . moderate-impact and high-impact information at rest and in transit."[33] To determine which impact level to apply to information, the National Institute of Standards and Technology suggests users consider multiple factors, including: how identifiable the information is; the sensitivity of the information both individually and aggregately; and the sensitivity given the purpose of collecting the information.[34] Transmission of a social security number alone is sufficient to trigger moderate-impact protocols and, therefore, the encryption requirement.[35] The social security number aggregated with other information predictably warrants additional security protocols.

---

[32] Hearing Before the H. Comm. on Elections, 87th Leg., 2018 Sess. (Kan. Jan. 10, 2018) (statement of Kris W. Kobach).

[33] Office of Mgmt. & Budget, Cir. A–130, *Managing Information as a Strategic Resource*, App'x I 13, 22–23 (2016). Information has a moderate impact if the potential "loss of confidentiality . . . could be expected to have a serious adverse effect on . . . individuals." (A serious adverse effect involves the threat of significant financial or non-life-threatening harm.). Nat'l Inst. of Standards and Tech., Dep't of Com., *FIPS 199: Standards for Security Categorization of Federal Information and Information Systems*, at 2 (2004). A high potential impact entails a "severe or catastrophic adverse effect", which is defined as one that might result in major financial loss, life-threatening injuries, or loss of life. *Id.* at 3.

[34] Nat'l Inst. of Standards and Tech., Dep't of Com., Spec. Publ'n 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 3–2 to 3–5 (2010).

[35] *Id.* at 3–3.

64. Similarly, the Kansas Information Technology Executive Council (KITEC), which is responsible for approval and maintenance of all information technology policies for government agencies, has promulgated minimum technology security requirements.[36] These requirements state that all restricted-use information[37] must be protected from unauthorized disclosure and encrypted when electronically sent outside of a secure boundary.[38] KITEC's encryption requirement explicitly applies to information that "is not subject to public release by an entity in accordance with statute or court order,"[39] including partial social security numbers provided as part of voter registration.[40]

Defendant Kobach's Collection, Maintenance and Transmission Protocols as the Operator of Crosscheck

65. Defendant Kobach exposes the confidential personal information of Kansas voters through his data collection, maintenance, and transmission practices as the operator of Crosscheck.

66. On information and belief, Defendant Kobach emails usernames, login information, and decryption passwords, which would provide access to Crosscheck results files, in clear text in emails sent to dozens of recipients.

67. From 2012 through 2017, Defendant Kobach uploaded and extracted voter files through an unsecure FTP program. FTP is not a secure method of transmission without additional

[36] Kan. Info. Tech. Executive Council, Information Technology Policy 7230 Revision 2 - Information Technology Enterprise Security Policy (2014).
[37] 'Restricted-use information' includes sensitive personally identifiable information (PII), which is defined as "[a]ny non-public PII that 1) the data subject has not voluntarily disclosed, 2) is not subject to public release by an entity in accordance with statute or court order, or 3) an entity collected after notice to the data subject that the information is categorized for public release." Kan. Info. Tech. Executive Council, Information Technology Security Standard 7230A 2, ¶ 5.3, 5.5 (2014).
[38] *Id.* at 8, ¶¶ 11.3–.4 (2014).
[39] *Id.* at 2, ¶ 5.3, 5.5 (2014)
[40] Kan. Stat. Ann. § 25-2309(j) (West 2018); Kan. Stat. Ann. §75-3520 (West 2018). Notably, the Kansas Legislature recently amended § 75-3520 to require the redaction in public documents of any portion of a social security number. *See* S.B. 336, 87th Leg., § 9 (Kan. 2018) (effective July 1, 2018).

layers of security. On information and belief, the Crosscheck FTP server lacked a valid secure socket layer (SSL) certificate and was not fortified by secure shell (SSH) software.

68. Therefore, extraction files and results files containing Kansas voter personal identifying information and partial social security numbers were transmitted to and from the host server through an unsecure method.

69. In or around October 2017, Defendant Kobach began hosting the Crosscheck database on a server in the Kansas Secretary of State's office. On information and belief, the server continues to lack industry standard security protocols. For instance, the Crosscheck server currently only uses a single-factor authentication system, allowing potential access to the program without detection.[41]

70. Further, on information and belief, the database is linked to other Kansas government networks that are not password protected.[42]

Defendant Kobach's Maintenance and Transmission Protocols as a Participant in Crosscheck

71. Defendant Kobach exposes the confidential personal information of Kansas voters through his office's data collection, maintenance, and transmission practices as a Crosscheck participant.

72. On information and belief, Defendant Kobach has sent and continues to send voter personal identifying information and partial social security numbers as an unencrypted email attachment to other participant states.[43]

---

[41] Dell Cameron, *As Crosscheck Moves to Secure Voter Data, Hacking Fears Grow Among Experts and Politicians*, Gizmodo (Jan. 24, 2018), https://gizmodo.com/as-crosscheck-moves-to-secure-voter-data-hacking-fears-1822344007.

[42] *Id.*

[43] Email from Jameson Beckner, Kansas Assistant Director of Elections, to Maria Matthews, Florida Director of the Division of Elections (Apr. 29, 2013, 11:56 AM).

73. On information and belief, Defendant Kobach sends voter signatures as an unencrypted email attachment to other participant states.

74. Defendant Kobach directs counties to send voter personal identifying information and partial social security numbers as an unencrypted email attachment to other participant states.[44]

75. On information and belief, Defendant Kobach shares the confidential personal information of Kansas voters with states that could release voter information to the public in response to an open records request.

Defendant Kobach Declines to Share Voter Information with Election Integrity Commission Because He Believes It Would Violate State Law

76. On or about May 12, 2017, President Donald J. Trump appointed Defendant Kobach to serve as the Vice-Chair of the Presidential Advisory Commission on Election Integrity.

77. On or about June 28, 2017, Defendant Kobach sent a letter to himself and election officials in 49 other states requesting "the publicly-available voter file data for [your state], including, if publicly available under the laws of your state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information."

78. Defendant Kobach directed himself and other election officials to "submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File

[44] *See, e.g.* Email from Rick Piepho, Deputy Clerk and Election Officer of Harvey County, Kansas, to the Florida Division of Elections (Aug. 14, 2013, 9:28 AM).

Exchange ('SAFE'), which is a secure FTP site the federal government uses for transferring large data files."

79. On or about July 3, 2017, House Minority Leader Jim Ward wrote a letter to Kansas Attorney General Derek Schmidt requesting an opinion about "whether the Secretary of State may disclose to the federal government [certain voter registration information absent voter consent.]"[45]

80. On or about July 11, 2017, the Attorney General issued an opinion stating that "the Secretary of State is forbidden to release the last four digits of a voter's Social Security number submitted as part of a voter registration and must redact that information from any records that may be released [to the public.]"[46] Attorney General Schmidt also opined that the Presidential Advisory Commission on Election Integrity was a "person" under the state's open records law, and any information shared with the Commission was tantamount to releasing information to the public.[47]

81. Defendant Kobach publicly stated that he would not share voter's partial social security numbers with the Commission, stating "In Kansas, the Social Security Number is not publicly available." However, Defendant Kobach stated that it *may* be legal to share voter's partial social security number with the Commission if Kansas uploaded the information, stating "[i]f the commission decides that they would like to receive Social Security numbers to a secure site in order to remove false positives, then we would have to double check and make sure Kansas law permits."[48]

---

[45] Kan. Att'y Gen. Op. No. 17-10 at 1–2 & n. 1 (July 11, 2017), http://ag.ks.gov/docs/default-source/ag-opinions/2017/2017-010.pdf?sfvrsn=bf29d51a_6.
[46] *Id.* at 3.
[47] *Id.* at 2 n. 2.
[48] Bryan Lowry, *Kobach: Kansas Won't Give Social Security Info to Kobach-led voter commission at this time*, Kansas City Star (July 1, 2017), http://www.kansascity.com/news/politics-government/article159113369.html.

States Express Concerns about Defendant Kobach's Security and Transmission Protocols

82. Participants repeatedly expressed concerns that voters' partial social security numbers would be subject to release by certain participant states under open records laws.

83. According to Caskey, half of the states participating in Crosscheck do not provide voters' partial social security number in their extraction file. When Florida participated in Crosscheck, the Director of the Division of Elections declined to provide voter social security information because Defendant Kobach was unable to ensure that voter SSNs would not be subject to release in response to an open records request.[49]

84. FDE suggested that Defendant Kobach create and share a list of the information that is closed from disclosure under each participant states' laws in order to prevent disclosures.[50]

85. Defendant Kobach declined to adopt this practice despite his staff's acknowledgment that "have been concerned about [records requests] for several years" and "would like to find firmer legal footing for denying these requests."[51]

86. On information and belief, at least four states have left Crosscheck or suspended their participation in the program over concerns about Defendant Kobach's ability to maintain the security of private voter information.

87. According to a survey, New York left Crosscheck, in part, because "there was no guarantee [that social security numbers] would be private."[52]

---

[49] Email from Maria Matthews, Florida Director of the Division of Elections, to Brad Bryant, former Kansas Elections Director (Oct. 23, 2013, 8:58 PM).
[50] Email from Maria Matthews, Florida Director of the Division of Elections to Brad Bryant, former Kansas Director of Elections (Oct. 29, 2013, 12:27 PM).
[51] Email from Brad Bryant, former Kansas Director of Elections, to Maria Matthews, Florida Director of the Division of Elections (Oct. 29, 2013, 2:51 PM).
[52] *See* Illinois Survey Results, Inter-State Cross Check and ERIC Participation: Individual Responses, https://www.surveymonkey.com/results/SM-FCJWLBZ5/ (comment to question 3 by respondent 24).

88. A tweet posted by Kentucky's Secretary of State Allison Grimes suggested that Kentucky withdrew from Crosscheck because of Defendant Kobach's inability to protect voter data from public disclosure. Linking a story about Defendant Kobach's release of voter and state employee social security numbers, Grimes wrote, "Another example of why KY doesn't participate in KS #Crosscheck program[.]"[53]

89. Illinois and Idaho have both publicly stated that they will not send information to Crosscheck until Defendant Kobach can guarantee the security of voter data.

Plaintiff Scott Moore's Information Is Exposed

90. Plaintiff Scott Moore is a forty-six-year-old United States citizen residing in Mission Hills, Kansas. Moore first registered to vote in Kansas in 1992 when he was attending the University of Kansas in Douglas County. He re-registered in 1998 after moving to Johnson County.

91. Moore is registered as an unaffiliated or "independent" voter. He has voted in every general election contested in Kansas since 1992.

92. In 2013, Defendant Kobach compared Moore's information with voter data submitted from Alaska, Alabama, Arizona, Arkansas, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana, Kentucky, Michigan, Mississippi, Missouri, Nebraska, Ohio, Oklahoma, Tennessee, Virginia, and Washington.

93. Moore shares a birthdate with a man named Scott Moore who lives in Naples, Florida. As a result Plaintiff Moore was one of the 945 voters identified as potential double registrants by Defendant Kobach in 2013.

[53] Alison Grimes (@AlisonForKY), Twitter (Jan. 25, 2018, 4:34 PM), https://twitter.com/AlisonForKY/status/956686808477261824.

94. Defendant Kobach sent the list of potential double registrants, including Plaintiff Moore to FDE as an unencrypted email attachment on April 29, 2013.

95. In November 2017, the FDE released Defendant Kobach's email containing the name, date of birth, address, and partial social security number of 945 Kansas voters, including that of Plaintiff Moore. The exposed information was viewable because Defendant Kobach's office shared the information as an unencrypted attachment to an email sent to FDE.

96. Moore learned about the disclosure of his information in or around November 2017 when his neighbor Anita Parsa, who had received the list from Florida in response to an open records request, contacted him.

97. In or around March 2018, Moore received a letter from the FDE offering him a year-long subscription to Lifelock.

Plaintiff James Long's Information is Exposed

98. James Long is a seventy-four-year-old U.S. citizen and Navy veteran who resides in Topeka, Kansas.

99. Long first registered to vote in Kansas in 1961 and has never registered to vote in another state. He has lived in Shawnee County for most of his life, except for several years while he was serving in the Navy.

100. Long has voted in every Presidential election in Kansas since 1964. He also has voted in the majority, if not all, of the state and municipal elections contested in Topeka, Kansas since 1990.

101. In 2013, Defendant Kobach compared Long's information with voter data submitted from Alaska, Alabama, Arizona, Arkansas, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana,

Kentucky, Michigan, Mississippi, Missouri, Nebraska, Ohio, Oklahoma, Tennessee, Virginia, and Washington.

102. Long shares a birthdate with a man named James Long who lives in South Palm Beach, Florida. As a result Plaintiff Long was one of the 945 voters Defendant Kobach identified as potential double registrants in 2013.

103. Defendant Kobach sent the list of potential double registrants, including Long to the Florida Division of Elections as an unencrypted email attachment on April 29, 2013.

104. In November 2017, FDE released the name, date of birth, address, and partial social security number of 945 Kansas voters, including that of Long. The exposed information was viewable because Defendant Kobach's office shared the information as an unencrypted attachment to an email sent to FDE.

105. Long does not recall receiving a letter from FDE notifying him about the disclosure. He also does not recall receiving an offer for a year-long subscription to Lifelock.

Plaintiff Nancy Perry's Information is Exposed

106. Nancy Perry is a sixty-one-year-old U.S. citizen who resides in Topeka, Kansas.

107. Perry registered to vote in Kansas in 2005. She is registered as an "independent" or "unaffiliated" voter and has voted in every general election contested in Kansas since 2010.

108. Perry has not lived or registered to vote in another state since registering in Kansas in 2005. She has never lived in or registered to vote in Florida.

109. In 2013, Defendant Kobach compared Perry's information with voter data submitted from Alaska, Alabama, Arizona, Arkansas, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana, Kentucky, Michigan, Mississippi, Missouri, Nebraska, Ohio, Oklahoma, Tennessee, Virginia, and Washington.

110. Perry shares a birthdate with a woman named Nancy Perry who lives in Osceola County, Florida. As a result Plaintiff Perry was one of the 945 voters identified as potential double registrants by Defendant Kobach in 2013.

111. Defendant Kobach sent the list of potential double registrants, including Perry to FDE as an unencrypted email attachment on April 29, 2013.

112. In November 2017, FDE released the name, date of birth, address, and partial social security number of 945 Kansas voters, including that of Plaintiff Perry. The exposed information was viewable because Defendant Kobach's office shared the information as an unencrypted attachment to an email sent to FDE.

113. In or around March 2018, Perry received a letter from the Florida Department of State notifying her that her social security number had been exposed. The letter also offered Perry a year-long subscription to Lifelock if she enrolled before April 21, 2018. Perry was confused about how the Florida Secretary of State would have been in possession of her social security number. Because Perry believed she may have mistakenly received the letter and wanted to get more information, she did not enroll prior to the April 21st deadline.

Florida Division of Elections Releases Plaintiffs Voter Information in Response to Open Records Request

114. On or about November 20, 2017, FDE released over 200 emails in response to an open records request submitted by Anita Parsa concerning Florida's participation in Crosscheck.

115. One email from Defendant Kobach to the Florida Division of Elections included attachments of unencrypted documents containing Kansas voters' partial social security numbers and personal identifying information. The documents were not password

protected. Further, Defendant Kobach failed to redact the partial social security number of the 945 Kansas voters listed in the document.

116. FDE produced a second email from Harvey County Election Clerk Rick Piepho that included a pdf attachment of the Kansas Voter Registration application of a resident of Newton, Kansas. The voter's name, address, driver's license number, phone number, and partial social security number were all listed. The pdf attachment was not encrypted. Moreover, the attachment was not password protected. The clerk also failed to redact the voter's partial social security number.

Voters Learn About Disclosure

117. On information and belief, in or around late March 2018, FDE mailed letters to Kansas voters who had their information publicly disclosed in response to Parsa's open records request, including Plaintiffs Scott Moore and Nancy Perry.

118. The letter notified voters that their partial social security number had been disclosed and offered a complimentary year-long subscription to Lifelock identity theft protection services. The letter provided no information as to how the disclosure occurred or why Florida had sensitive information of Kansas residents in its possession.

119. The subscription would have provided Kansas voters with stolen funds reimbursement benefits up to $25,000, identity restoration support services, and an identity theft alert system.

120. Voters were required to subscribe for the service over the phone by April 21, 2018 in order to be eligible for the offer.

Claims for Relief

Count 1
Violation of Fourteenth Amendment: Right to Informational Privacy

(Claims of Named Plaintiffs and Class Members Pursuant to 42 U.S.C. §1983 Against Defendant Kobach for Violations of Fourteenth Amendment)

121. Plaintiffs repeat and re-allege paragraphs 1-120.

122. The Federal Constitution protects Plaintiffs from the public disclosure of their personally identifying information. *See* U.S. Const. amend XIV; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977); *Kerns v. Bader*, 663 F.3d 1173, 1186 (10th Cir. 2011); *Sheets v. Salt Lake County*, 45 F.3d 1383, 1388 (10th Cir. 1995).

123. Defendant, by failing to adopt adequate safeguards to prevent the Plaintiffs' partial social security numbers and sensitive personal information from being released to the public, has violated the informational privacy rights of Plaintiffs and hundreds of other Kansans.

124. Further, Defendant has violated the right of informational privacy of Plaintffs and hundreds of other Kansans through its actual disclosure of their partial social security number and other personally identifiable information.

125. Defendant Kobach, acting under the color of state law, has created and maintained inadequate security protocols in the maintenance and sharing of voter registration data, causing unwarranted disclosures of private voter information and creating a demonstrable risk of future releases.

126. Declaratory and injunctive relief is required to remedy continuing violations of Plaintiffs' right to information privacy and to prevent future exposures.

Count 2

Violation of the Public Records Act

(Claims of Named Plaintiffs and Class Members against Defendant Kobach, in his individual capacity, for Violation of the Kansas Public Records Act)

127. Plaintiffs repeat and re-allege paragraphs 1-126.

128. K.S.A. §75-3520 prohibits the disclosure and inspection of any document containing a social security number where the document also contains an individual's personal information, including their name, address, phone number, or email address.

129. Defendant Kobach, acting under the Color of State Law, disclosed Plaintiffs' name, address, date of birth, and partial social security number in violation of K.S.A. §75-3520. Further, sharing Plaintiffs' private information with Florida and other states who would be required to release the information in response to an open records request under their open records law constitutes a public release under K.S.A. §75-3520.

130. Declaratory relief as well as the assessment of civil penalties, pursuant to K.S.A §75-3520, is necessary to remedy past violations of Plaintiff's rights under and prevent future disclosures.

Prayer for Relief

131. Wherefore, Plaintiff respectfully requests that this Court:

a. Enter judgement in favor of Plaintiffs and against Defendants, adjudging Defendant's policies and actions to be unconstitutional, and holding Defendants liable to Plaintiffs;

b. Enter a declaratory judgement in favor of Plaintiffs, adjudging that, by failing to maintain adequate safeguards to prevent the public disclosure of sensitive personal information, Defendant violated Plaintiffs' Fourteenth Amendment Right to privacy, as well as Plaintiffs' rights under the Kansas Public Records Act;

c. Issue an injunction requiring Defendant to halt transmission of personal voter data until industry standard practices and procedures are implemented;

d. An assessment of civil penalties pursuant to K.S.A. §75-3520 (c) against Defendant, in his individual capacity, for each violation of the Act;

e. Award Plaintiffs the costs and reasonable attorneys' fees incurred in this action;

f. Grant such other relief as the Court may deem just and proper.

Designation Place of Trial

Pursuant to D. Kan. 40.2, Plaintiff designates Kansas City, Kansas as the place of trial.

Respectfully submitted,

/s/ Lauren Bonds
Lauren Bonds, KS Sup. Ct. No. 27807
ACLU Foundation of Kansas
6701 W. 64th St., Suite 210
Overland Park, KS 66202
Phone: (913) 490-4100
Fax: (913) 490-4119
lbonds@aclukansas.org

/s/ Mark P. Johnson
Mark P. Johnson, KS Sup.Ct. No. 22289
Dentons US LLP
4520 Main Street, Suite 1100
Kansas City, MO 64111
Phone: (816) 460-2400
Fax: (816) 531-7545
mark.johnson@dentons.com