**IN THE 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,**<br><br>**Plaintiffs,**<br><br>**v.**<br><br>**KRIS KOBACH, in his individual capacity, and SCOTT SCHWAB, in his official capacity as the Secretary of State of Kansas,**<br><br>**Defendants.** | **Case No. 18-2329-DDC-KGG** |

## MEMORANDUM AND ORDER

Before the court is defendants Kris Kobach and Scott Schwab's Motion to Dismiss (Doc. 11).[1] It presents two vexing questions of constitutional law: Does the Constitution recognize a right to informational privacy? And, if so, does that right prohibit public disclosure of purportedly private voter information? Regrettably, the Supreme Court has not decided either one of these questions. And though our Circuit has decided the first question, it has not addressed the second one. Consistent with Circuit precedent, the court concludes that such a right exists and, though it is a close question, the court holds that the Complaint's allegations plead a plausible claim for relief. The pages that follow explain why.

The court emphasizes that two procedural requirements play a prominent part in these conclusions. One, the questions come to the court on a motion to dismiss. The standard for

[1] As a matter of judicial housekeeping, the court substitutes plaintiffs' official capacity claim against defendant Kobach for an official capacity claim against his successor in that office—current Kansas Secretary of State Scott Schwab. Fed. R. Civ. P. 25(d).

surviving such a motion is a relatively forgiving one. Two, the court must assume that the "facts" pleaded in the Complaint are true, and view them in the light favoring plaintiffs. While the court applies that standard in this Order, it does not imply that plaintiffs ultimately will prove their version of the facts is true. Time will tell.

## I. Overview

Before describing the facts that control the current motion, the court briefly summarizes the case's overarching legal issue.

The Constitution does not explicitly recognize a right to informational privacy. On this everyone agrees. But a trilogy of Supreme Court decisions has assumed, without deciding, that such a right exists. *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457–65 (1977); *Whalen v. Roe*, 429 U.S. 589, 598–99 (1977). Recognizing constitutionally protected "zones of privacy," the Court has opined that this right—if it indeed exists—includes an individual's interest not to have their personal matters disclosed publicly. *See Whalen*, 429 U.S. at 598–99.

Whether the Constitution recognizes a right to informational privacy is a dispositive question for plaintiffs' official capacity claim. Here, plaintiffs Scott Moore, James Long, and Nancy Perry bring this lawsuit, on behalf of themselves and all others similarly situated, against defendant Kris Kobach. They have sued defendant Kobach in his individual capacity and official capacity as Kansas Secretary of State. Defendant Kobach no longer serves as Kansas Secretary of State, so, by rule, current Kansas Secretary of State Scott Schwab becomes the defendant on the official capacity claim. Fed. R. Civ. P. 25(d).

Plaintiffs' two claims take aim at the Interstate Voter Registration Crosscheck Program ("Crosscheck"), a data comparison program used to compare voter registration information

among participating states. The Kansas Secretary of State's ("KSOS") Office runs Crosscheck. In Count One, the Complaint alleges that the Kansas Secretary of State—acting in his official capacity—has violated their Fourteenth Amendment right to informational privacy in two ways: (1) failing to adopt adequate safeguards for Crosscheck; and (2) disclosing part of plaintiffs' Social Security numbers and other personally identifiable information. And, because plaintiffs allege these constitutional violations are continuing ones, they seek injunctive and declaratory relief requiring the KSOS to stop exchanging plaintiffs' voter data until the KSOS can ensure their information will not be subject to public disclosure. In Count Two, plaintiffs allege that defendant Kobach—in his individual capacity—has violated the Kansas Public Records Act ("KPRA"). Plaintiffs seek civil penalties on their KPRA claim.

Defendants filed a Motion to Dismiss both claims under Fed. R. Civ. P. 12(b)(6). Doc. 11. Plaintiffs have filed a Response in Opposition. Doc. 14. And, defendants have submitted a Reply. Doc. 15. After considering the parties' arguments the court denies the Motion to Dismiss for reasons explained, below.

## II. Facts

As referenced above, the court must accept the facts asserted in the Complaint as true, and view them in the light most favorable to plaintiffs. *Burnett v. Mortg. Elec. Registration Sys., Inc.*, 706 F.3d 1231, 1235 (10th Cir. 2013) (citing *Smith v. United States*, 561 F.3d 1090, 1098 (10th Cir. 2009)). The following facts thus come from plaintiffs' Complaint (Doc. 1).

### A. The Interstate Voter Registration Crosscheck Program

Former Kansas Secretary of State Ron Thornburg launched Crosscheck in 2005 to help Kansas and neighboring states compare voter data and detect double registrants. The KSOS Office administers Crosscheck by collecting voter registration information from participant states

and cross-referencing lists for potential matches. The KSOS then generates reports listing potential duplicate records for each participating state.

Crosscheck uses a two-point match criteria, identifying registered voters who share the same first name, last name, and date of birth. Participating states also are asked to provide additional voter data, including part of the 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. In 2017, at least 10 states did not provide partial Social Security numbers for the KSOS to use to narrow results of the program's cross-checking.

Crosscheck participants principally share data through a File Transfer Protocol ("FTP") website, which the Arkansas Secretary of State's Office previously hosted. The KSOS now hosts this site. Participants share data with the KSOS by uploading their voter rolls to the FTP site. Specifically, each participant state extracts voter data from its registration rolls and formats that information to coincide with the formatting used by Crosscheck for data. The participating states then encrypt their files using a free encryption program and upload the data to the FTP site. Before 2017, defendant Kobach used the AxCrypt software to encrypt files; plaintiffs allege that 7-zip, another free encryption program, is now used.

Participating states are asked to upload their data each January. Once they upload their extraction files, the KSOS pulls the files from the FTP site, runs a comparison of each state's voter information, and uploads result files to the FTP site. The KSOS then notifies each state that its results file is available and emails a decryption passphrase enabling the state to open its results file. The results file contains a potential match list, which identifies voters registered in that state who share a name and date of birth with a voter in another state. Once states have received their potential match lists, they may contact the other state where the voter, at least

potentially, is double registered. When processing potential match results, the KSOS advises participating states to procure the voter's middle name, a partial Social Security number, and signature to help determine whether the voter has registered to vote in more than one state.

Each state participating in Crosscheck is directed to inform the KSOS about its preferred method for communicating information requests. While the Crosscheck participation guide cautions against transmitting personally identifiable information about voting registrants via e-mail, no provision of the Memorandum of Understanding ("MOU") restricts unsecured transmissions. Plaintiffs allege that the MOU contains the only requirements governing states' participation in Crosscheck.

### B. Defendants' Policies and Practices for Requesting and Transmitting Information

As a participant in Crosscheck, the KSOS analyzes potential matches by comparing secondary data about voters. Secondary data includes voters' partial Social Security numbers and middle initials. Once the KSOS narrows the number of potential matches, it submits information requests to the other state where double voting may have occurred. The KSOS provides the name and date of birth of potential match voters to the other participating states and requests documentation about voting history and the voter's signature in the other state. Plaintiffs allege that the KSOS requests states to supply voter signatures as unencrypted email attachments. Plaintiffs also allege that the KSOS lacks a method to narrow potential matches when the other participating state does not provide a partial Social Security number or a middle initial. So, plaintiffs contend, when a state does not include partial Social Security numbers or middle initials in its extraction file, the KSOS maintains a practice of sending full potential match lists in unencrypted email attachments to the other participant state. These full match lists include partial Social Security numbers and other personal identifying information about

hundreds of voters. About half the states participating in Crosscheck provide partial Social Security numbers.

### C. States Begin to Join Crosscheck

From 2005 to 2011, Crosscheck had just four participating states: 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." Doc. 1 at 18. In 2012, 10 new states joined Crosscheck, expanding the number of participants to 14 states. By 2016, 30 states participated in Crosscheck. So, plaintiffs allege, in 10 years Crosscheck's participants increased from four to 26 states and 100 million voter records were added to its comparison database. Despite this increase in the number of participating states and voter records, defendant Kobach never developed a more sophisticated protocol for sharing potential matches or ensuring that states maintained the shared voter data in a secure fashion. Also, defendant Kobach downsized his IT staff after the program expanded.

### D. Industry Standard Protocols for Data Maintenance and Transmission

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." Doc. 1 at 19. The National Institute of Standards and Technology suggests multiple factors to determine the "impact level" of information. They include the following factors: how identifiable the information is; how sensitive the information is, both individually and in the aggregate; and how sensitive the information is, given its purpose. Under these factors, transmitting one Social Security number by itself is sufficient to trigger moderate-impact protocols and, therefore, an encryption requirement. The aggregation and transmission of Social Security numbers with other information warrants additional security protocols.

Similarly, the Kansas Information Technology Executive Council (KITEC)—which is responsible for approving and maintaining all information technology policies for Kansas's governmental agencies—has promulgated minimum technology security requirements. KITEC's minimum standards mandate that users protect all restricted-use information from unauthorized disclosure and encrypt such information when sending it outside a secure boundary. 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," including partial Social Security numbers provided as part of voter registration. *Id.* at 20.

### E. Defendants' Collection, Maintenance, and Transmission Protocols as the Operator of Crosscheck

Plaintiffs allege that defendant Kobach, as Crosscheck's operator, exposed the confidential personal information of Kansas voters by his practice of collecting, maintain, and transmitting data. On information and belief, plaintiffs allege that defendant Kobach sent usernames, login information, and decryption passwords (which provide access to Crosscheck results files) in clear text emails to dozens of recipients.

From 2012 to 2017, defendant Kobach uploaded and extracted voter files by using an unsecure FTP. Plaintiffs allege that Crosscheck's FTP is not a secure method of transmission, and it lacks additional layers of security. Also, plaintiffs allege that Crosscheck's FTP server lacked a valid secure socket layer ("SSL") certificate and was not fortified by secure shell ("SSH") software. So, extraction files and results files containing personal identifying information about Kansas voters and partial Social Security numbers were transmitted to and from the host server by unsecure methods.

At some point in or near October 2017, defendant Kobach began hosting the Crosscheck database on a server operated in the KSOS's Office. Plaintiffs allege that the server lacked and

still lacks industry standard security protocols. For example, currently, the Crosscheck server uses a single-factor authentication system. This kind of system allows access to the Crosscheck program without detection. And, plaintiffs allege, Crosscheck's database is linked to other Kansas governmental networks that are not password protected.

### F. Defendants' Maintenance and Transmission Protocols as a Participant in Crosscheck

As a Crosscheck participant, defendant Kobach exposed the confidential personal information of Kansas voters by collecting, maintaining, and transmitting their data. Plaintiffs allege that defendant Kobach has sent voters' personal identifying information, partial Social Security numbers, and voter signatures as unencrypted email attachments to other participating states. Plaintiffs allege this exposure is ongoing. Also, plaintiffs allege defendant Kobach directed counties to send voters' personal identifying information and partial Social Security numbers as unencrypted email attachments to other participating states. Last, plaintiffs allege that defendant Kobach shared confidential personal information about Kansas voters with other states who could release that personal voter information to the public in response to open records requests.

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

On May 12, 2017, President Donald J. Trump appointed defendant Kobach to serve as Vice-Chair of the Presidential Advisory Commission on Election Integrity. And, on June 28, 2017, defendant Kobach addressed 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 information in another state, information regarding military status, and overseas citizen information." Doc. 1 at 22. Defendant Kobach directed himself and the other election officials to "submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files." *Id.* at 22–23.

On July 3, 2017, Kansas House Minority Leader Jim Ward sent a letter to Kansas Attorney General Derek Schmidt. This letter requested an opinion "whether the Secretary of State may disclose to the federal government [certain voter registration information without voter consent]." *Id.* at 23. The Attorney General issued his opinion on or around July 11, 2017. It opined 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]." *Id.* Attorney General Schmidt also opined that the Presidential Advisory Commission on Election Integrity was a "person" for purposes of the Kansas Open Records Act, and any information shared with the Commission was tantamount to releasing the information to the public.

Defendant Kobach publicly stated that he would not share voters' partial Social Security numbers with the Commission, asserting that "[i]n Kansas, the Social Security number is not publicly available." *Id.* But, defendant Kobach claimed that it may be legal to share voters' partial Social Security number with the Commission if Kansas uploaded the information. He asserted, "If 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" it. *Id.*

### H. States Express Concern About Defendant Kobach's Security and Transmission Protocols

States participating in Crosscheck expressed concerns that voters' partial Social Security numbers would be subject to release by other participating states under certain state open records laws. According to Kansas Elections Director Brian Caskey, half of the states participating in Crosscheck do not provide voters' partial Social Security numbers in their extraction files. When Florida participated in Crosscheck, the Director of the Florida Division of Elections ("FDE") declined to provide Social Security information because defendant Kobach could not ensure that the voters' Social Security numbers would not be subject to release in response to an open records request. The FDE suggested that defendant Kobach create and share a list of the information closed from disclosure under each participating state's laws. Defendant Kobach declined to implement this practice even though his staff acknowledged that it "[has] been concerned about [records requests] for several years," and "would like to find firmer legal footing for denying those requests." *Id.* at 24.

Plaintiffs allege that at least four states either have left or stopped participating in Crosscheck based on concerns about defendant Kobach's ability to secure private voter information. According to a survey, New York left Crosscheck, in part, because "there was no guarantee [that Social Security numbers] would be private." *Id.* And, Kentucky Secretary of State Allison Grimes suggested that Kentucky withdrew from Crosscheck because defendant Kobach could not protect voter data from public disclosure: Secretary Grimes linked a story about defendant Kobach's release of voter and state employee Social Security numbers. She also wrote, "Another example of why KY doesn't participate in KS #Crosscheck program[.]" Illinois

and Idaho both have stated publicly that they will not send information to Crosscheck until defendant Kobach can guarantee the voter data's security.

## I. Plaintiffs' Voter Information is Disclosed

### 1. Scott Moore

Plaintiff Scott Moore is a 46-year-old United States citizen living in Mission Hills, Kansas. Mr. Moore first registered to vote in Kansas in Douglas County in 1992, while attending the University of Kansas. He re-registered to vote in 1998 after moving to Johnson County. Mr. Moore is registered as an unaffiliated, or "independent" voter. He has voted in every general election contest in Kansas since 1992.

In 2013, defendant Kobach compared Mr. 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.

Mr. Moore shares a birthdate with a man named Scott Moore, who lives in Naples, Florida. As a result, Mr. Moore was one of 945 voters who defendant Kobach identified as potential double registrants in 2013. On April 29, 2013, defendant Kobach sent the list of potential double registrants, a list that included Mr. Moore, to the FDE in an unencrypted email attachment. In November 2017, the FDE released defendant Kobach's email containing the name, date of birth, address, and partial Social Security number of 945 voters. This disclosure included Mr. Moore's information. Others could view the exposed information because defendant Kobach's office shared the information in an unencrypted attachment to an email sent to the FDE.

In November 2017, Mr. Moore learned that his information was disclosed from his neighbor, Anita Parsa. Ms. Parsa had received the list from Florida in response to an open records request, and she contacted Mr. Moore. And, in March 2018, Mr. Moore received a letter from the FDE offering him a year-long subscription to Lifelock.

**2. James Long**

Plaintiff James Long is a 74-year-old United States citizen. He is a Navy veteran living in Topeka, Kansas. Mr. Long first registered to vote in Kansas in 1961 and never has registered to vote in another state. He has lived in Shawnee County for most of his life, except for several years while he served in the Navy. Mr. 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 conducted in Topeka, Kansas, since 1990.

In 2013, defendant Kobach compared Mr. 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.

Mr. Long shares a birthdate with a man named James Long, who lives in South Palm Beach, Florida. As a result, Mr. Long was one of 945 voters who defendant Kobach identified as a potential double registrant in 2013. On April 29, 2013, defendant Kobach sent the list of potential double registrants, a list that included Mr. Long, to the FDE in an unencrypted email attachment. In November 2017, the FDE released defendant Kobach's email containing the name, date of birth, address, and partial Social Security number of 945 voters. This disclosure included Mr. Long's information. Others could view the exposed information because defendant

Kobach's office shared the information in an unencrypted attachment to an email sent to the FDE.

Mr. Long does not recall receiving a letter from the FDE notifying him that his information was disclosed. Also, he does not recall receiving an offer for a year-long subscription to Lifelock.

**3. Nancy Perry**

Nancy Perry is a 61-year-old United States citizen living in Topeka, Kansas. In 2005, Ms. Perry registered to vote in Kansas. She is registered as an "independent" or "unaffiliated" voter and has voted in every general election in Kansas since 2010. Ms. Perry has not lived or registered to vote in another state since registering in Kansas in 2005. She never has lived in or registered to vote in Florida.

In 2013, defendant Kobach compared Ms. 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.

Ms. Perry shares a birthdate with a woman named Nancy Perry who lives in Osceola County, Florida. As a result, Ms. Perry was one of the 945 voters defendant Kobach identified as a potential double registrant in 2013. On April 29, 2013, defendant Kobach sent the list of potential double registrants, a list that included Ms. Perry, to the FDE in an unencrypted email attachment. In November 2017, the FDE released defendant Kobach's email. It contained the name, date of birth, address, and partial Social Security number of 945 voters, including Ms. Perry's information. Others could view the exposed information because defendant Kobach's office shared the information in an unencrypted attachment to an email sent to the FDE.

In March 2018, Ms. Perry received a letter from the Florida Department of State notifying her that her Social Security number was exposed. The letter also offered Ms. Perry a year-long subscription to Lifelock if she enrolled before April 21, 2018. Ms. Perry was confused why the Florida Secretary of State would have possessed her Social Security number. Because Ms. Perry believed she may have received the letter mistakenly and wanted to get more information, she did not enroll before the April 21 deadline.

### J. Florida Division of Elections Releases Plaintiffs' Voter Information in Response to an Open Records Request

On November 20, 2017, the Florida Division of Elections released more than 200 emails in response to an open records request submitted by Anita Parsa about Florida's participation in Crosscheck. One email that defendant Kobach had sent to the FDE included attachments of unencrypted documents. These documents contained partial Social Security numbers and personal identifying information about Kansas voters. The documents were not password protected. Also, defendant Kobach failed to redact the partial Social Security numbers of the 945 Kansas voters identified in the document.

The FDE also produced a second email from Harvey County, Kansas Election Clerk Rick Piepho. This email included a PDF attachment of the Kansas Voter Registration application for a resident of Newton in Harvey County, Kansas. This attachment divulged the voter's name, address, driver's license number, phone number, and partial Social Security number. The PDF attachment was neither encrypted nor password protected. The Election Clerk also had failed to redact the voter's partial Social Security number.

### K. Voters Learn About the Disclosure

Plaintiffs allege that, in March 2018, the FDE mailed letters to Kansas voters whose information had been disclosed publicly in response to Ms. Parsa's open records request.

Plaintiffs Moore and Perry received the FDE's letter. The FDE's letter notified the Kansas voters that part of their Social Security numbers had been disclosed and offered them a complimentary year-long subscription to Lifelock identity theft protection services. The letter did not explain how the disclosure had occurred or why Florida possessed sensitive information about Kansas residents. The Lifelock subscription would have provided the Kansas voters with reimbursement benefits worth $25,000, identity restoration support services, and an identity theft alert system. To receive the Lifelock subscription, the Kansas voters had to subscribe for the service over the phone no later than April 21, 2018.

## III. Legal Standard

Fed. R. Civ. P. 8(a)(2) requires a complaint to contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Although this Rule "does not require 'detailed factual allegations,'" it demands more than "'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action'" which, as the Supreme Court explained, simply "will not do." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

"To survive a motion to dismiss [under Fed. R. Civ. P. 12(b)(6)], a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Id.* (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). "Under this standard, 'the complaint must give the court reason to believe that *this* plaintiff has a reasonable likelihood of mustering factual support for *these* claims.'" *Carter v. United States*,

667 F. Supp. 2d 1259, 1262 (D. Kan. 2009) (quoting *Ridge at Red Hawk, L.L.C. v. Schneider*, 493 F.3d 1174, 1177 (10th Cir. 2007)).

Although the court must assume that a complaint's factual allegations are true, it is "not bound to accept as true a legal conclusion couched as a factual allegation." *Id.* at 1263 (quoting *Iqbal*, 556 U.S. at 678). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to state a claim for relief. *Bixler v. Foster*, 596 F.3d 751, 756 (10th Cir. 2010) (quoting *Iqbal*, 556 U.S. at 678).

## IV. Allegations Made "Upon Information and Belief"

Before the court addresses defendants' substantive arguments, it first considers defendants' argument that the court should ignore several allegations asserted—the Complaint says—based "upon information and belief." Doc. 15 at 2. Specifically, defendants contest paragraphs 55, 56, 69, 70, 72, 73, 75, and 86 of the Complaint because "allegations made 'upon information and belief' are conclusory allegations which are not accepted as true, unless the complaint also alleges specific facts which form the basis of the belief." *Id.* (first citing *Jackson-Cobb v. Sprint United Mgmt.*, 173 F. Supp. 3d 1139 (D. Colo. 2016); then citing *Montoya v. O'Friel*, No. 17 CV 693 JAP/JHR, 2017 WL 5891757, at *7 (D.N.M. Nov. 27, 2017)).

Defendants ask the court to exclude any allegation shrouded in the buzz words "information and belief," yet they never explain why this Complaint fails to support those allegations with specific facts. *See Jackson-Cobb*, 173 F. Supp. 3d at 1149 ("The Tenth Circuit has held in various contexts that allegations, even allegations of fraud, may be made on information and belief so long as the complaint sets forth the factual basis of the belief." (citing *Schiedt v. Klein*, 956 F.3d 963, 967 (10th Cir. 1992))). The question, then, is not whether the allegation uses the words, "information and belief." Instead, the question is whether such

allegations are supported by specific facts asserted by the Complaint. Close review of the disputed allegations in this Complaint reveals that specific facts support the challenged allegations.

As an example, plaintiffs allege "On information and belief, [that] Kansas requests states to supply voter signatures as an unencrypted email attachment." Doc. 1 at 17 (Compl. ¶ 55); *see also id.* at 21 (Compl. ¶ 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."). For support, plaintiffs append a footnote to each statement. And, that footnote includes part of an email from Jameson Beckner, Kansas Assistant Director of Elections, to Maria Matthews, Florida Director of the Division of Elections. *Id.* at 17 (Compl. ¶ 55 n.28) ("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.)"). The court concludes that specific facts alleged in the cited email support these allegations sufficiently.

The other allegations challenged by defendants' argument follow a similar pattern. The Complaint alleges "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." Doc. 1 at 18 (Compl. ¶ 56); *but see id.* (Compl. ¶ 57 n.29) (citing email from Mr. Beckner stating, "I didn't know of any other way to really examine if any double votes occurred between [Kansas and Florida] without middle initial or SSN to narrow the results.").

Also, the Complaint alleges "On information and belief, the server continues to lack industry standard security protocols." Doc. 1 at 21 (Compl. ¶ 69). The next sentence provides the factual basis for this assertion: "For instance, the Crosscheck server currently only uses a single-factor authentication system, allowing potential access to the program without detection." *Id.*; *see also id.* at 4 (Compl. ¶ 10) ("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.").

And, the Complaint alleges, "on information and belief, [that] the database is linked to other Kansas government networks that are not password protected." Doc. 1 at 21 (Compl. ¶ 70). The Complaint alleges that defendants began hosting the Crosscheck data on a server in the KSOS's Office, and that the server lacks industry standard security protocols. Doc. 1 at 21 (Compl. ¶ 69). The Complaint further alleges, "Defendant Kobach's office maintained a practice of emailing the server URL and encryption passwords in plain text, [and] the audit revealed that any reader of the emails would easily be able to access and download voter records." Doc. 1 at 5 (Compl. ¶ 10).

Last, defendants contest the sufficiency of these allegations: "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[,]" Doc. 1 at 21 (Compl. ¶ 72); "On information and belief, Defendant Kobach sends voter signatures as an unencrypted email attachment to other participant states[,]" Doc. 1 at 21 (Compl. ¶ 73); and, "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[,]" Doc. 1 at 21 (Compl. ¶ 75). But the Complaint

lends factual support to these allegations with specific facts: "In November 2017, the Florida Department of State Division of Elections . . . released the name, date of birth, address, and partial social security number of 945 Kansas voters, including that of the Plaintiffs. The exposed information was shared by Defendant Kobach's office as an unencrypted attachment to an email sent to FDE." Doc. 1 at 6 (Compl. ¶ 14).

Defendants' "information and belief" argument is unpersuasive. The court thus rejects defendants' request to exclude these allegations from the facts accepted as true for purposes of the current motion.

## V. § 1983 Right to Informational Privacy Claim

"To state a claim under § 1983, a plaintiff must allege the violation of a right secured by the Constitution and laws of the United States, and must show that the alleged deprivation was committed by a person acting under color of state law." *West v. Atkins*, 487 U.S. 42, 48 (1988) (citations omitted); *Northington v. Jackson*, 973 F.2d 1518, 1523 (10th Cir. 1992). Plaintiffs here allege that the Fourteenth Amendment recognizes a right to informational privacy. And, plaintiffs allege, the KSOS has deprived them of that right by failing to adopt adequate security procedures for the Crosscheck program—*i.e.*, by sharing plaintiffs' Crosscheck profiles with other states without proper security measures. In sum, plaintiffs claim that defendant Kobach has allowed—and defendant Schwab continues to allow—public disclosure of plaintiffs' private data.

Before addressing this argument, the court returns to the distinction between plaintiffs' Complaint—which brought official and individual capacity claims against defendant Kobach—and the current procedural status now that defendant Kobach no longer serves as Kansas Secretary of State. Fed. R. Civ. P. 25(d) provides that an "action does not abate when a public

officer who is a party in an official capacity . . . ceases to hold office while the action is pending. Instead, "[t]he officer's successor is automatically substituted as a party." *Id.*; *see also Lamb v. Norwood*, 262 F. Supp. 3d 1151, 1154 n.2 (D. Kan. 2017). Scott Schwab replaced defendant Kobach as Kansas Secretary of State in January 2019. Consistent with Rule 25(d), the court substitutes Mr. Schwab as the correct defendant on plaintiffs' official capacity claim, which seeks declaratory and injunctive relief for ongoing violations of their constitutional right to informational privacy. The court thus turns to defendant Schwab's official capacity arguments.

Defendant Schwab's motion to dismiss the official capacity claim relies on two arguments. First, he contends, qualified immunity bars plaintiffs' claim from proceeding. Second, defendant Schwab contends that there is no constitutional right to informational privacy; and so, without a constitutional right, defendant cannot be liable under § 1983. The court addresses each argument, in turn, below.

**A. Qualified Immunity**

As Section V.B explains, significant uncertainty exists about the substance of the law governing plaintiffs' § 1983 claim. *See Lesier v. Moore*, 903 F.3d 1137, 1141 (10th Cir. 2018) ("[T]he Supreme Court has made clear that the existence of such a right [to informational privacy] is an open question and it has not abandoned a third precedent which suggests that any right to informational privacy is limited."). It would seem, therefore, that qualified immunity would apply. But, qualified immunity can't apply because plaintiffs' § 1983 claim does not seek to recover damages from defendant Schwab. Doc. 14 at 13. "Under the *Ex Parte Young* doctrine, the Eleventh Amendment generally does not bar a suit against a state official in federal court which seeks only prospective equitable relief for violations of federal law, even if the state is immune. Thus, because plaintiffs in this case name state officers as defendants and seek only

prospective injunctive relief, it seems to fit squarely within the traditional application of *Ex parte Young*." *J.B. ex rel. Hart v. Valdez*, 186 F.3d 1280, 1286 (10th Cir. 1999) (internal citations and quotations omitted). Here, plaintiffs have named a state officer as the only defendant on the official capacity claim and only seek prospective injunctive relief on that claim. The court thus concludes qualified immunity does not apply to the kind of § 1983 claim asserted in this action.

### B. The Existence of a Constitutional Right to Privacy

The motion to dismiss also asks the court to dismiss the Complaint because it fails to state a claim. This argument relies on a single premise: The Constitution never establishes a right to informational privacy. *See* Doc. 12 at 3–4; Doc. 15 at 2–4. Defendant Schwab's Memorandum relies primarily on just two cases to support this argument: *NASA v. Nelson*, 562 U.S. 134 (2011), and *Leiser v. Moore*, 903 F.3d 1137 (10th Cir. 2018). Doc. 12 at 4; Doc. 15 at 2–4. This approach is far too narrow. And this argument misreads at least one of the two cited cases.

Below, in Section V.B.1, the court outlines the Supreme Court's intermittent analysis of this controlling legal issue. This part of the discussion includes the KSOS's lead case—*NASA*. Finding no controlling answer in any Supreme Court case, the court turns to decisions from our Circuit in Part V.B.2. This part of the analysis addresses the second case relied on by defendant—*Leiser*. For reasons it explains, Part V.B.2 concludes that our Circuit has recognized the right posited by the Complaint—"a right not to have one's private affairs made public by the government." Finally, in Section V.B.3, the court briefly evaluates the Complaint's allegations in light of the Circuit authority. Section V.B.3's analysis is abbreviated because defendant Schwab's Memorandum never argues that the Complaint's allegations are deficient. He just

argues that the right doesn't exist. In sum, the court denies defendant Schwab's motion because its basic premise is wrong.

### 1. Supreme Court Precedent

While the Constitution never explicitly establishes a right to informational privacy, several Supreme Court cases have grappled with the question whether such a right exists. As Justice Alito termed it, "[i]n two cases decided more than 30 years ago," the Supreme Court "referred broadly to a constitutional privacy 'interest in avoiding disclosure of personal matters.'" *NASA*, 562 U.S. at 138 (first citing *Whalen v. Roe*, 429 U.S. 589 (1977); then citing *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425 (1977)). Believing the two cases cited by Justice Alito's opinion in *NASA* provide important context, the court discusses them extensively, below. The court then turns to the Supreme Court's most recent treatment of the right—in *NASA*. This discussion also explains why defendant Schwab's Memorandum misapprehends the case.

#### a. *Whalen v. Roe*

In *Whalen v. Roe*, the Supreme Court considered a constitutional challenge to the New York State Controlled Substances Act of 1972. 429 U.S. 589 (1977). This Act was designed to address concerns that wrongdoers were diverting drugs properly prescribed for therapeutic purposes to persons who abused these drugs. A state commission found no existing means to prevent the use of stolen or revised prescriptions, or to prevent doctors from over-prescribing such drugs. The New York legislature responded with the 1972 Act. It divided drugs into five categories, and one of them—Schedule II drugs—"include[d] the most dangerous of the legitimate drugs." *Id.* at 692–93. The Act required physicians to prepare all prescriptions for Schedule II drugs in triplicate and supply one copy of such prescriptions to New York's Department of Health.

Health Department personnel then sorted, coded, and logged data about Schedule II prescriptions onto magnetic tapes processable by a computer. The Act required the Health Department to retain the prescription forms themselves in a vault for five years and then, destroy them. Also, New York's health department stored the data about Schedule II prescriptions on computer tapes kept in a locked cabinet; access to the data was limited to 17 specified Department of Health employees. And even those 17 employees could access the data only by using a computer running unconnected to any other computer. The Act also conferred authority on 24 investigators to access the data when the computer's program identified possible "overdispensing." *Id.* at 595. The evidence presented to the district court established that statutorily authorized investigators had accessed the Schedule II data on a limited basis. In the 20 months following the act's effective date, they had accessed the data just twice. *Id.*

A group of patients who regularly received prescriptions for Schedule II drugs, the doctors prescribing those drugs, and associations of physicians and pharmacists sued. At trial, their evidence showed that some patients needing treatment with Schedule II drugs "will from time to time decline such treatment." *Id.* at 595. According to plaintiffs' evidence, those patients feared that misuse of computerized data "will cause [Schedule II patients] to be stigmatized as 'drug addicts.'" *Id.*

The district court enjoined the part of the Act requiring physicians to supply patients' names and addresses. *Id.* at 596. It reasoned that "the doctor-patient relationship intrudes on one of the zones of privacy accorded constitutional protection and that the patient-identification provisions of the Act invaded this zone with a needlessly broad sweep . . . ." *Id.* The Supreme Court reversed. Three aspects of Justice Stevens's opinion, issued for a unanimous court, matter to the current lawsuit.

*One*, *Whalen*'s holding deftly avoided the need to decide whether the Constitution recognizes a right to privacy. Justice Stevens expressed the case's holding this way: "We hold that neither the immediate nor the threatened impact of the patient-identification requirements in [the Act] is sufficient to constitute an invasion of *any right or liberty protected by the Fourteenth Amendment*." *Id.* at 603–04 (emphasis added). The rest of his opinion followed suit. It referred repeatedly to the privacy theory advanced by plaintiffs and noted, at most, that "the cases" and "[l]anguage in prior opinions of the Court" provided some support for plaintiffs' theory. *Id.* at 598 n.23, 599; *see id.* at 598–99 ("[Plaintiffs] contend that the statute involves a constitutionally protected zone of privacy. The cases sometime characterized as protecting privacy have in fact involved at least two kinds of interests. One is the individual interest in avoiding disclosure of personal matters. . . .") (internal quotation marks and footnotes omitted); *id.* at 598 n.23 ("As the basis for the constitutional claim [plaintiffs] rely on the shadows cast by a variety of provisions in the Bill of Rights. Language in prior opinions of the Court or its individual Justices *provides support for the view* that some personal rights implicit in the concept of ordered liberty are so fundamental that an undefined penumbra *may provide* them an independent source of constitutional protection.") (internal quotation marks and citations omitted) (emphasis added).

*Two*, *Whalen* envisioned the very circumstance at the heart of plaintiffs' theory here, but emphasized that the court was not deciding that case. "A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Id.* at 605. The court then provided examples—citing programs that collected taxes, distributed welfare and Social Security benefits, and enforced criminal laws—that "require[d] the orderly preservation of great quantities of information, much of which is personal in character and

potentially embarrassing or harmful if disclosed." *Id.* The Court noted, however, that the New York Act "evidence[d] a proper concern with, and protection of, the individual's interest in privacy." *Id.* And then, the Court explicitly declined to express any view about legislative acts that allegedly omitted measures demonstrating such a "proper concern." "We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not establish comparable security provisions." *Id.* at 605–06.

*Three*, *Whalen*'s two concurring opinions likely explained why the Court decided the case on an "assumed right" basis—the rationale used by Justice Stevens's opinion. Justice Brennan's concurring opinion explicitly emphasized his view that the Constitution protects a person's interest in avoiding disclosure of personal matters, calling it an aspect of the constitutional right to privacy. *See id.* at 606 (Brennan, J., concurring). He concluded, "Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests." *Id.* Justice Stewart's opinion couldn't disagree more. In effect, Justice Stewart's concurring opinion dissents from Justice Brennan's concurring opinion: "[A]lthough the Constitution affords protection against certain kinds of government intrusions into personal and private matters, there is no general constitutional right to privacy." *Id.* at 608 (Stewart, J., concurring). In Justice Stewart's view, protection of a person's right to privacy is "left largely to the law of the individual States." *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 350–51 (1967)).

### *b. Nixon v. Administrator of General Services*

Four months after deciding *Whalen*, the Supreme Court discussed informational privacy rights again in *Nixon v. Administrator of General Services*. 433 U.S. 425 (1977). In that case, former President Nixon had sued to challenge the Presidential Recordings and Materials Preservation Act. He contended that this Act abrogated an agreement he had made with the Administrator of General Services. The agreement governed custody and access to 42 million pages and 880 tape recordings of presidential records amassed during the Nixon presidency. Claiming the Act violated his privacy rights, President Nixon sued in federal court and sought specific performance of his agreement with the Administrator. The trial court consolidated the former President's suit with several other lawsuits that, on various theories, sought access to and possession of the disputed presidential materials. Those theories included the Presidential Recordings Act. President Nixon attacked that Act's validity under several constitutional theories, including his argument that the Act violated his rights to informational privacy. *Id.* at 429, 455. The district court rejected all of the former President's arguments, holding that the Act was not facially unconstitutional. *Id.* at 456.

A sharply divided Supreme Court affirmed in a 132-page opinion, with Justice Brennan writing the opinion of the court. Given his concurring opinion in *Whalen*, it came as no surprise that Justice Brennan began with a muted tribute to privacy rights. "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters . . . .'" *Id.* at 457 (quoting *Whalen*, 429 U.S. at 599) (majority opinion). Justice Brennan then explained that former Presidents, when they establish presidential libraries, "have usually withheld matters concerned with family or personal finances, or have deposited such materials with restrictions on

their screening." *Id.* This, he reasoned, gave rise to President Nixon's "legitimate expectation of privacy in the disputed material." *Id.* at 458.

The Court nonetheless rejected the former President's privacy challenge to the Records Preservation Act. It explained that the Court must evaluate the privacy challenge "in light of the specific provisions of the Act, and any intrusion must be weighed against the public interest in subjecting the Presidential materials of [his] administration to archival screening." *Id.* Deeming President Nixon's privacy interest "weaker than that found wanting [in *Whalen*]," *id.*, the Court rejected President Nixon's privacy claim.

In doing so, *Nixon* used the same rubric as *Whalen*. The Court again declined to decide whether the Constitution establishes a right to informational privacy. "We may assume . . . for purposes of this case, that this pattern of de facto Presidential control and congressional acquiescence gives rise to [President Nixon's] legitimate expectation of privacy in such materials." *Id.* at 457. In short, *Nixon* assumed such a constitutional right exists but held that the public interest in preserving presidential records outweighed any constitutional right to informational privacy. *Id.* at 465.

In short, Justice Brennan's *Nixon* opinion refers broadly to an interest "in avoiding disclosure of personal matters." *Id.* at 457. Some of the concurring opinions are similar. But one cannot fairly read the case to establish a Constitution-based right of privacy against disclosure of personal matters.

c. ***NASA v. Nelson***

The uncertainty of *Whalen* and *Nixon* persisted, at least at the Supreme Court level, until 2011 and *NASA v. Nelson*. 562 U.S. 134 (2011). *NASA* described the state of the question this way: "Since [*Nixon*], the Court has said little else on the subject of an 'individual interest in

avoiding disclosure of personal matters.' A few opinions have mentioned the concept in passing and in other contexts. But no other decision has squarely addressed a constitutional right to informational privacy." *Id.* at 146 (citations and footnote omitted).

In *NASA*, 28 employees of the Jet Propulsion Lab ("JPL")—a facility where all unstaffed space missions from 1958 to 2001 were developed—sued NASA. Though NASA owned the JPL, the California Institute of Technology ("Cal Tech") operated it under a government contract. So, employees who worked at JPL were Cal Tech employees, including the case's 28 plaintiffs. They objected to a new federal mandate requiring them to complete the same governmental background investigation as NASA employees. Specifically, this background check required Cal Tech employees to respond to a questionnaire asking if they had used, supplied, or possessed illegal drugs during the last year. And, if so, the questionnaire required them to provide details and disclose any treatment or counseling for recent drug use. *Id.* at 138. Also, the background check used a second questionnaire. It was distributed to former employers, landlords, schools, and others identified in the employee's response to the first questionnaire.

The federal Privacy Act applied to both questionnaires. The Privacy Act permitted the government to retain the completed questionnaires but only as necessary to accomplish an end required by law. *See* 5 U.S.C. § 522a(e). And subject to specified exceptions, governing law forbade the government from disclosing the completed questionnaires without the employee's written consent. § 522a(b).

Shortly before the deadline for submitting completed questionnaires, the 28 Cal Tech employees sued in federal court. They claimed that the background check violated a constitutional right to informational privacy. The district court denied plaintiffs' request for a preliminary injunction but the Ninth Circuit reversed. It held that parts of both questionnaires

likely were unconstitutional and should be enjoined. The Ninth Circuit reasoned that many of the inquiries were not problematic, but the questions about illegal drugs required closer scrutiny. Ultimately, the Ninth Circuit held, the questions about employees' recent involvement with drugs furthered a legitimate governmental interest. But it also held that other questions—ones requiring disclosure of drug treatment or counseling—furthered no legitimate interest and thus likely were unconstitutional. *NASA*, 562 U.S. at 143. Over five dissents, the Circuit denied rehearing en banc and the Supreme Court granted certiorari.

Justice Alito authored the opinion of the Court. His analysis began by discussing the unsettled question identified in the two 1977 cases—*Whalen* and *Nixon*. He closed this retrospective by observing that no Supreme Court case had "squarely addressed" a claimed constitutional right to informational privacy. *Id.* at 146.

Justice Alito's next sentence ended any suspense, and terminated any possibility that *NASA* would answer the constitutional ambiguity lingering since 1977. He wrote: "As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance. We hold, however, that whatever the scope of this interest, it does not prevent the Government from asking reasonable questions of the sort" included in the challenged questionnaires. *Id.* at 147–48.

Notwithstanding *NASA*'s explicit holding, the motion to dismiss argues that *NASA* supplies proof positive that the Constitution recognizes no right to informational privacy. And without such a right, he argues, the Complaint can assert no plausible claim. *See* Doc. 15 at 2–4. Specifically, the motion to dismiss cites Justice Scalia's concurring opinion in *NASA* as the source of the result defendant attaches to the case. *Id.* at 3. One deficiency in this argument is evident immediately. Justice Scalia's opinion is a concurring opinion. It does not announce the

opinion of the Court. And cursory attention to the content of Justice Scalia's opinion reveals more deficiencies.

Early in his concurring opinion, Justice Scalia explained his view: "I agree with the Court, of course, that background checks of employees of government contractors do not offend the Constitution. But rather than reach this conclusion on the basis of the never-explained assumption that the Constitution requires courts to 'balance' the Government's interests in data collection against its contract employees' interest in privacy, I reach it on simpler grounds . . . A federal constitutional right to 'informational privacy' does not exist." *NASA*, 562 U.S. at 159–60 (Scalia, J., concurring). In sum, Justice Scalia directly explained how he would have preferred for the Court to decide *NASA*. But in doing so, he exposed the error of the KSOS's current argument, *i.e.*, that *NASA* excludes the right that the Complaint here seeks to vindicate.

Justice Thomas's concurring opinion merely emphasizes the point. He wrote, "I agree with Justice Scalia that the Constitution does not protect a right to informational privacy." *Id.* at 169 (Thomas, J., concurring). But in agreeing with Justice Scalia, he recognized that the other Justices had not reached that conclusion in *NASA*.

**d. Conclusion about Supreme Court Precedent**

In sum, the court finds no controlling answer in *Whalen*, *Nixon*, or *NASA*. To the contrary, the Supreme Court's most recent authority establishes that the Court hasn't yet decided whether the Constitution recognizes a right to informational privacy. With this conclusion in hand, the court turns to this court's other source of controlling authority: the Tenth Circuit.

**2. Tenth Circuit Precedent**

Fortunately, summarizing the precedent from our Circuit is a simpler task. Last year, a published decision from the Tenth Circuit explained the current state of the question in the Tenth

Circuit: "In two published opinions this circuit has held governmental disclosure of an individual's personal medical information violated the Constitution." *Leiser v. Moore*, 903 F.3d 1137, 1140 (10th Cir. 2018) (first citing *Herring v. Keenan*, 218 F.3d 1171, 1173 (10th Cir. 2000); then citing *A.L.A. v. West Valley City*, 26 F.3d 989, 990 (10th Cir. 1994)). But the analysis can't end there, for *Leiser* also recognizes some questions about the viability of the Circuit's earlier holdings.

*Lesier* referenced "the development—or, perhaps more precisely, the clarification—of the relevant constitutional law by the Supreme Court in the interval between our precedents and this case." *Id.* at 1142. In context, this "interval" refers to Supreme Court decisions that post-date *A.L.A.* and *Herring*. The Circuit then explained, "More recently, however, the Supreme Court has made clear that the existence of such a right is an open question and it has not abandoned a third precedent which suggests that any right to informational privacy is limited." *Id.* *Leiser* then referenced the Supreme Court decisions in *Whalen*, *Nixon*, and a third Supreme Court case—*Paul v. Davis*, 424 U.S. 693 (1976).[2]

The Circuit then focused on the "development" that had raised legitimate questions about the right to informational privacy. This review began with *Connecticut Department of Public Safety v. Doe*, 538 U.S. 1 (2003), a case where the Supreme Court—according to *Leiser*—had

[2] In *Paul*, police chiefs had circulated a flyer to merchants that included plaintiff's name and photo, identifying him as an "Active Shoplifter." *Paul*, 424 U.S. at 694–95. The flyer identified the plaintiff because he had been arrested on a charge of shoplifting, but he had not been convicted. *Id.* at 695–96. Plaintiff then filed a § 1983 claim against the police chiefs.

Relevant here is the *Paul* plaintiff's allegation that the police chiefs violated his "right to privacy guaranteed by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments." *Id.* at 712. The Court rejected this argument, reasoning that its "right of privacy" cases envelop "rights found in this guarantee of personal privacy" that "must be limited to those which are 'fundamental' or 'implicit in the concept or ordered liberty[.]'" *Id.* at 713 (quoting *Palko v. Connecticut*, 302 U.S. 319, 325 (1937)). The *Paul* plaintiff claimed constitutional protection against the disclosure of his shoplifting arrest, but the Court found this theory exceeded its precedent, which recognized protections for "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education." *Id.*

"recognized that there was at least some life left in *Paul*." The Circuit then turned to the case that it viewed as "[m]uch more important[]" than *Doe—NASA v. Nelson*. *Lesier*, 903 F.3d at 1143. *Leiser* viewed *NASA* to establish the proposition "that any statements in [Supreme Court] precedents regarding a constitutional protection against government disclosure of personal information were dicta." *Id.* The Circuit concluded this discussion by recognizing that some language in its own precedents no longer could stand. For instance, *Leiser* reasoned *NASA* plainly nullified *A.L.A.*'s observation that "[t]here is no dispute that confidential medical information is entitled to constitutional privacy protection." *Id.* at 1144.

But this is as far *Leiser* goes. Contrary to the argument here, *Leiser* stops short of overruling existing Circuit authority. Indeed, the Circuit used words that contradict defendant's argument: "This"—referring to *Leiser*'s recognition that the Supreme Court had said it is an "open question" whether such a constitutional right exists—"is not to say that our precedents on this issue are incorrect or that they have been overruled." *Id.*

The Circuit did surmise that one way to square its informational privacy precedents—at least in the context of private medical information disclosures—was to ask whether the government action shocks the conscience. *Id.* ("For example, it would be consistent with our precedents to say that disclosures are prohibited only when they shock the conscience." (citing *Browder v. City of Albuquerque*, 787 F.3d 1076, 1078–79 (10th Cir. 2015)). The Circuit found that it was not clearly established whether the Supreme Court would reject the distinction between a government's disclosure of a cancer diagnosis vis-a-vis disclosure of an HIV diagnosis, as the Second Circuit had done in *Matson v. Board of Education*, 631 F.3d 57 (2d Cir. 2011). *See id.* at 1145 ("[The Second Circuit] declared that 'the interest in the privacy of medical information will vary with the condition'" (quoting *Matson*, 631 F.3d at 64)). By

concluding that the law was not "clearly established" on this question, *Lesier* affirmed the trial court's qualified immunity ruling. *Id.* at 1145.

But the issue presented by the motion to dismiss in the current case is not as forgiving. The court cannot decide that motion simply by ruling that the law isn't "clearly established." Instead, to rule on defendant's motion, the court must decide—straight up or down—whether the Tenth Circuit precedent recognizes a right to informational privacy. On that issue, the court finds nothing in *Leiser* to overrule the holdings in *Herring* and *A.L.A.* The court is duty-bound, of course, to follow existing authority. *United States v. Spedalieri*, 910 F.3d 707, 709 n.2 (10th Cir. 1990) ("A district court must follow the precedent of this circuit, regardless of its views concerning the advantages of the precedent of our sister circuits.") (citations omitted); *see also In re Smith*, 10 F.3d 723, 724 (10th Cir. 1993) ("We are bound by the precedent of prior panels absent en banc reconsideration or a superseding contrary decision by the Supreme Court."). Consistent with that duty, the court holds that existing Tenth Circuit precedent recognizes a right to informational privacy. The court thus rejects the argument that this constitutional right no longer exists in our Circuit.

### C. Plaintiffs Have Stated a Plausible Claim That Defendant Schwab Continues to Violate Their Right to Informational Privacy

The motion to dismiss never argues that, if a constitutional right to privacy exists, plaintiffs have failed to satisfy the Tenth Circuit's two-part standard for asserting such a claim. But, "[t]o survive a motion to dismiss [under Fed. R. Civ. P. 12(b)(6)], a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The court thus briefly considers whether plaintiffs have pleaded sufficient facts to

state a plausible claim that defendant Schwab continues to violate their right to informational privacy.

They have, at least for now at the motion to dismiss stage. In the Tenth Circuit, courts employ a two-prong test. First, the information must be entitled to a legitimate expectation of confidentiality. "Information falls within the ambit of constitutional protection when an individual has a 'legitimate expectation . . . that it will remain confidential while in the state's possession.'" *Sheets v. Salt Lake Cty.*, 45 F.3d 1383, 1387 (10th Cir. 1995). (citing *Mangels v. Pena*, 789 F.2d 836, 839 (10th Cir. 1986)). In *Sheets*, our Circuit explained that the "legitimacy of this expectation depends 'at least in part, upon the intimate or otherwise personal nature of the material which the state possesses.'" *Id.* (quoting *Mangels*, 789 F.2d at 839). But, the "information need not be embarrassing to be personal," and thus fall within the protection of the Fourteenth Amendment. *Id.* As examples, the Circuit noted that "medical and certain financial records . . . have [been] placed within the ambit of constitutional protection." *Id.* (first citing *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir. 1980); then citing *Fraternal Order of Police, Lodge 5 v. Philadelphia*, 812 F.2d 105, 115 (3d Cir. 1987)). Second, "[i]f an individual has a legitimate expectation of confidentiality, then '[d]isclosures of such information must advance a compelling state interest, which, in addition must be accomplished in the least intrusive manner.'" *Id.* (quoting *Mangels*, 789 F.2d at 839) (further citation omitted).

Turning to the first requirement—whether plaintiffs plead facts giving rise to a plausible claim that they are entitled to a legitimate expectation of privacy in their Crosscheck data—our Circuit never has held that the disclosure of partial Social Security numbers, coupled with full names, addresses, and birth dates, implicates a constitutional right of privacy. But, plaintiffs cite persuasive law from other jurisdictions in support of such a theory, at least with respect to full

Social Security numbers. *See, e.g.*, *Greidinger v. Davis*, 988 F.2d 1344, 1354 (4th Cir. 1993) ("Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous."); *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999) ("[T]he indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses, may implicate the constitutional right to informational privacy.").

Although these cases do not bind this court, they are persuasively reasoned. And so, the court finds it plausible that plaintiffs have pleaded facts sufficient to establish a reasonable expectation of confidentiality in their Crosscheck data. Plaintiffs allege that defendant exposed a spreadsheet identifying the name, address, date of birth, and partial Social Security number for 945 voters. Based on these cases, the court predicts that the Tenth Circuit would find—as a matter of law—that the Crosscheck files in this case are "highly personal and intimate" and trigger an expectation of privacy. The court recognizes the issue isn't one-sided. It is possible that the Circuit could reach the opposite conclusion. But though the boundaries of the right remain in flux, plaintiffs have the better of the argument for now. *See Leiser*, 903 F.3d at 1144.

To state a valid *Ex parte Young* claim, plaintiffs also must plead facts alleging an ongoing violation of their informational right to privacy. Plaintiffs carry their burden. Plaintiffs allege that the KSOS deliberately has disclosed their personal data to the FDE as part of the Crosscheck program, which was then publicly disclosed. And, plaintiffs allege, defendant Schwab continues to send plaintiffs' Crosscheck data to states where this information can be disclosed to the public through open records request, in part, because of defendant Schwab's failure to take adequate security precautions. The court thus finds that plaintiffs have stated a plausible claim for prospective injunctive relief.

The court now turns to the second requirement of the analysis: Did disclosing plaintiffs' Crosscheck data advance a compelling state interest, and, if so, was it accomplished in the least intrusive manner? Defendant never addressed this question. *See Sheets*, 45 F.3d at 1387 (noting that defendants provided no reason why disclosure was warranted when detective shared plaintiff's wife's diary with third party author, who ultimately published diary excerpts in book). In short, the briefing made to support the motion fails to provide the kind of cogent analysis that a motion to dismiss requires. Given the absence of meaningful argument or analysis, the court presumes that the disclosures did not serve a compelling state interest, and was not done in the least intrusive manner. The court thus holds that plaintiffs have pleaded facts sufficient to state an informational privacy claim.

## VI. Kansas State Law Claim

Count Two of the Complaint alleges that defendant Kobach is liable in his individual capacity for violations of a Kansas state statute. The Kansas statute provides, "Unless required by federal law, no document available for public inspection or copying shall contain an individual's social security number if such document contains such individual's personal information. 'Personal information' shall include, but not be limited to, name, address, phone number or e-mail address." Kan. Stat. Ann. § 75-3520(a)(1). The statute also mandates that "[a]ny document or record that contains *all or any portion of an individual's social security number* shall have all portions of all social security numbers redacted before the document or record is made available for public inspection or copying." *Id.* § 75-3520(a)(3). When a state agency discovers an unauthorized disclosure, it must give individual notice and offer individualized credit monitoring services at no cost for one year. *Id.* § 75-3520(a)(4)(A)–(B).

And, aggrieved individuals "may recover a civil penalty of not more than $1,000 for each violation." *Id.* § 75-3520(c).

Defendant Kobach's motion makes both jurisdictional and substantive attacks on this claim. Because federal courts are courts of limited jurisdiction, the court addresses the subject matter jurisdiction arguments first. After concluding that it has jurisdiction over this state law claim, the court then addresses defendant Kobach's substantive arguments.

**A. Jurisdictional Arguments**

Defendant Kobach makes two jurisdictional arguments. First, defendant Kobach contends that no federal question jurisdiction exists under 28 U.S.C. § 1331 because there is no constitutional right to informational privacy. And, without federal question jurisdiction, the court cannot exercise supplemental jurisdiction under 28 U.S.C. § 1367(a). As explained in Section V, the court has concluded that *NASA* and *Leiser* do not foreclose a constitutional right to informational privacy. The court thus concludes it has federal question jurisdiction over plaintiffs' § 1983 claim and, by extension, supplemental jurisdiction over the state law claim under 28 U.S.C. § 1367(a).

Second, defendant Kobach asks the court to decline to exercise supplemental jurisdiction over plaintiffs' state law claims if the court dismisses plaintiffs' federal claim. The court has not dismissed plaintiffs' federal claim, and so it will not decline to exercise supplemental jurisdiction.[3]

[3] The court also concludes that the Eleventh Amendment and the Supreme Court's decision in *Pennhurst State School & Hospital v. Halderman*, 465 U.S. 89 (1984), do not prevent the court from exercising jurisdiction. *See, e.g.*, *Williams v. Kentucky*, 24 F.3d 1526, 1543 (6th Cir. 1994), *cert. denied*, 513 U.S. 947 (1994) ("[N]either the Eleventh Amendment nor *Pennhurst* deprives federal courts of jurisdiction over state law claims for damages against state officials sued in their individual capacities."); *Bad Frog Brewery, Inc. v. N.Y. State Liquor Auth.*, 134 F.3d 87, 102 (2d Cir. 1998) ("The jurisdictional limitation recognized in *Pennhurst* does not apply to an individual capacity claim seeking damages against a state official, even if the claim is based on state law.") (first citing *Ying Jing Gan v. City of New York*, 996 F.2d 522, 529 (2d Cir. 1993); then citing *Wilson v. UT Health Ctr.*, 973 F.2d 1263, 1271 (5th Cir. 1992)).

### B. Substantive Arguments

"State law claims before a federal court on supplemental jurisdiction are governed by state law." *Time Warner Entm't Co., L.P. v. Everest Midwest Licensee, L.L.C.*, 381 F.3d 1039, 1044 (10th Cir. 2004) (citing *Olcott v. Delaware Flood Co.*, 327 F.3d 1115, 1126 (10th Cir. 2003)). Kansas state courts have not yet applied the provisions of Kan. Stat. Ann. § 75-3520. "Where the state's highest court has not addressed the issue presented, the federal court must determine what decision the state court would make if faced with the same facts and issue." *Bain v. IMC Glob. Operations, Inc.*, 236 F. App'x 423, 426 (10th Cir. 2007) (quoting *Oliveros v. Mitchell*, 449 F.3d 1091, 1093 (10th Cir. 2006)).

Plaintiffs allege that defendant Kobach violated Kansas state law by sending full match lists, which include voters' partial Social Security numbers and other personal identifying information, to other states participating in Crosscheck. Doc. 1 at 18 (Compl. ¶ 57). Plaintiffs cite Florida's indirect disclosure of one such match list to support their claim.[4] And, plaintiffs contend, by sharing these match lists with participating states, these documents become records available for public inspection and copying. In response, defendant Kobach argues, first, that plaintiffs fail to state a claim because the full match lists—such as the one sent from Kansas to

[4] Neither party notes that Kan. Stat. Ann. § 75-3520 did not protect disclosure of *partial* Social Security numbers when coupled with other personal information until July 1, 2018. Before that time, the statute prohibited disclosure of an individual's *full* Social Security number when coupled with personal information. *Compare* Kan. Stat. Ann. § 75-3520(a)(1) (2017), *added by* 2006 Kan. Sess. Laws 149, § 2 ("Unless required by federal law, no document available for public inspection or copying shall contain an individual's social security number if such document contains such individual's personal information.") *with* Kan. Stat. Ann. § 75-3520(a)(3) (2018), *added by* 2018 Kan. Sess. Laws 87, § 9 ("Any document or record that contains all or any portion of an individual's social security number shall have all portions of all social security numbers redacted before the document or record is made available for public inspection or copying."). So, disclosure by the KSOS to the Florida Department of Elections in 2013 would predate the revised statute. But, plaintiffs do allege that defendant Kobach maintained a continuing practice of sending full potential match lists—containing partial Social Security numbers and other personally identifying information—as unencrypted email attachments to other states. Whether the evidence will substantiate plaintiffs' claim remains to be seen—but, plaintiffs' allegation that defendant Kobach continued this practice beyond July 1, 2018, satisfies the motion to dismiss standard.

Florida in 2013—is not a "document available for public inspection or copying" under § 75-3520(a)(1). But, the court predicts the Kansas Supreme Court would conclude that full match lists qualify as a "document available for public inspection or copying" under the statute.

To reach this conclusion, the court finds—in the absence of Kansas case law—the reasoning of the Kansas Attorney General analogous and persuasive. The Attorney General opined that if the KSOS's Office shared the last four digits of a registered voter's Social Security number with the federal government—specifically, the Presidential Advisory Commission on Election Integrity—it would violate Kansas election law under Kan. Stat. Ann. § 25-2309(j). Kan. Att'y Gen. Op. No. 2017-10 (2017), at *2, *2 n.12, 2017 WL 2987177. Section 25-2309(j) employs similar language to Kan. Stat. Ann. § 75-3520. This statute provides, "No application for voter registration shall be made available for *public inspection or copying* unless the information required by subsection (b)(5) has been removed or otherwise rendered unreadable." Kan. Stat. Ann. § 25-2309(j) (emphasis added). Subsection (b)(5)—*i.e.*, the information to be removed—includes "the last four digits of the person's social security number[.]" *Id.* § 25-2309(b)(5).

And, in concluding that sharing the last four digits of a registered voter's Social Security number with the federal government would violate Kan. Stat. Ann. § 25-2309(j), the Attorney General also cited Kan. Stat. Ann. § 75-3520—the statute at issue here. Kan. Att'y Gen. Op. No. 2017-10 (2017), at *2, *2 n.12, 2017 WL 2987177. The Attorney General opined that § 75-3520 "also prohibit[s] the public dissemination of the entire Social Security number of an identifiable person . . . We think [this statute] reflect[s] a strong public policy to protect such highly personal information." *Id.* The court concludes that sharing partial Social Security numbers of identifiable voters under Kan. Stat. Ann. § 75-3520 implicates the same "strong public policy

interest" as Kan. Stat. Ann. § 25-2309(j). And, the slight variation that the KSOS allegedly shared this information with state governments, instead of the federal government, does not produce a different conclusion.

Second, defendant Kobach argues that § 75-3520(a)(2)(6) exempts KSOS filings from the requirements of § 75-3520(a)(1). Plaintiffs respond, arguing that, when read with the preamble, this exemption only applies to documents filed in the official records of a recorder of deeds or a court. *See* Kan. Stat. Ann. § 75-3520(a)(2) (". . . this subsection shall not apply to documents recorded in the official records of any recorder of deeds of the county or to any documents filed in the official records of the court . . . ."). The court predicts the Kansas Supreme Court would agree with plaintiffs' argument. Documents identified by § 75-3520(a)(2) mirror the type of documents one might file as an official record with any recorder of deed or court.[5] But, for the exemption to apply, the document must be part of the official record of a Recorder of Deeds or a court. Defendant Kobach does not argue that the full match lists of Crosscheck data are official documents of a Recorder of Deeds or a court. The court thus concludes that the Crosscheck data is not exempt, and this conclusion means plaintiffs have stated a plausible claim under Kan. Stat. Ann. § 75-3520.

[5] Compare the list of exemplar records in § 75-3520(a)(2)—(A) A consensual or nonconsensual lien; (B) an eviction record; (C) a judgment; (D) a conviction or arrest; (E) a bankruptcy; (F) a secretary of state filing; or (G) a professional license—with the list of official records maintained by the Sedgwick County Register of Deeds in *Data Tree*: "Uniform Commercial Code (UCC) filings including UCC releases or satisfactions; birth and death certificates; military discharges; federal and state tax liens and tax lien releases or satisfactions; mortgages and mortgage releases or satisfactions; various judgments or liens and releases or satisfactions thereof; various deeds, plats, and indexes; miscellaneous notices and affidavits; affidavits of equitable interests; bankruptcy, probate, and miscellaneous court documents; powers of attorney; and refiled, corrected documents. Many of these documents are likely to contain social security numbers, mothers' maiden names, and dates of births." *Data Tree, LLC v. Meek*, 109 P.3d 1226, 1230 (Kan. 2005).

## VII. Conclusion

Although it is difficult to draw the precise boundaries of a constitutional right to informational privacy when the boundaries remain in flux, the most recent controlling authority recognizes such a right. And under the legal standard adopted in this case authority, the Complaint states a plausible § 1983 against defendant Schwab for an ongoing violation of plaintiffs' Fourteenth Amendment right to informational privacy. The court also holds the Complaint states a plausible claim against defendant Kobach under Kan. Stat. Ann. § 75-3520. For those reasons, the court denies defendants' Motion to Dismiss. Doc. 11.

**IT IS THEREFORE ORDERED BY THE COURT THAT** defendants' Motion to Dismiss (Doc. 11) is denied.

**IT IS SO ORDERED.**

**Dated this 1st day of February, 2019, at Kansas City, Kansas.**

**s/ Daniel D. Crabtree**
**Daniel D. Crabtree**
**United States District Judge**