# IN THE COURT OF CRIMINAL APPEALS OF TENNESSEE AT KNOXVILLE

December 20, 2016 Session

# STATE OF TENNESSEE v. ALEXANDER JOHNSON AND MICHAEL F. WILLIAMS

Appeal from the Criminal Court for Knox County No. 104964A, B Bob McGee, Judge

No. E2015-02486-CCA-R9-CD - Filed April 12, 2017

In this interlocutory appeal, the defendants, Alexander Johnson and Michael F. Williams, challenge the ruling of the Knox County Criminal Court granting the State's motion to quash subpoenas duces tecum issued to four State's witnesses. The State challenges that portion of the court's ruling denying its motion to quash subpoenas duces tecum issued to various electronic communications service providers. Because the State lacks standing to challenge any of the subpoenas issued in this case, we reverse that portion of the court's ruling granting the State's motion to quash the subpoenas issued to the witnesses. We affirm that portion of the trial court's ruling that the State lacks standing to challenge the subpoenas issued to the service providers. In the interest of judicial economy and to facilitate further appellate review, we have examined the preempted issues related to the subpoenas duces tecum issued in this case and have concluded that: (1) although nothing prevents the defendants in this case, generally, from obtaining the type of electronic communications at issue via a subpoena issued under the terms of Tennessee Rule of Criminal Procedure 17 to the witnesses themselves, the defendants have failed to establish entitlement to all of the requested communications as discussed more fully below; and (2) under the terms of the Stored Communications Act, see 18 U.S.C. §§ 2701 - 2703, the defendants cannot obtain the contents of the electronic communications from any of the service providers via a Rule 17 subpoena duces tecum. Accordingly, the trial court's November 3, 2015 order relative to the subpoenas duces tecum issued in this case is affirmed in part and reversed in part. The case is remanded to the trial court for proceedings consistent with this opinion.

# Tenn. R. App. P. 3; Judgment of the Criminal Court Affirmed in Part; Reversed in Part; Remanded

JAMES CURWOOD WITT, JR., J., delivered the opinion of the court, in which THOMAS T. WOODALL, P.J., and NORMA MCGEE OGLE, J., joined.

Stephen Ross Johnson and W. Thomas Dillard, Knoxville, Tennessee, for the appellant, Alexander Johnson.

David Eldridge and Loretta G. Cravens, Knoxville, Tennessee, for the appellant, Michael F. Williams.

Herbert H. Slatery III, Attorney General and Reporter; Nicholas W. Spangler, Assistant Attorney General; Charme P. Allen, District Attorney General; and Leslie Nassios and Kyle Hixson, Assistant District Attorneys General, for the appellee, State of Tennessee.

### **OPINION**

On February 12, 2015, the Knox County Grand Jury charged both of the defendants with two counts each of the November 2014 aggravated rape of C.C.<sup>1</sup> As is relevant to this appeal, the presentment lists as witnesses C.C., Bridget Boland, and cellular telephone service providers New Cingular Wireless/AT&T Wireless and Sprint/Nextel Communications. Witnesses Anna Lawn and Natalie Tavares were later added to the presentment by order. The case proceeded, and discovery materials were exchanged by the parties.

On August 21, 2015, Mr. Johnson moved the trial court for an order to accompany subpoenas duces tecum for the production and pretrial inspection of "specified cellular telephone and social media communications and information." He argued that the "requested communications are evidentiary and relevant," that the communications were "not otherwise reasonably procurable in advance of trial by due dilligence," that he could not prepare for trial in the absence of this information, and that the motion was "made in good faith" and was "not intended as any general 'fishing expedition." In support of his motion, Mr. Johnson alleged that discovery materials already provided by the State "confirm[ed] the existence of social media information and communications material and relevant to the events at issue." He stated that interviews with several of the State's witnesses indicated that many of those witnesses, including C.C., had communicated with both of the defendants and with each other via text message, iMessage, and social media before and after the alleged offenses occurred.

<sup>&</sup>lt;sup>1</sup> We utilize initials in keeping with the policy of this court.

<sup>&</sup>lt;sup>2</sup> Mr. Williams later moved the court to adopt each of the relevant motions filed by Mr. Johnson.

<sup>&</sup>quot;You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS." https://support.apple.com/en-us/HT207006 (last visited February 1, 2017). "iMessages are texts, photos, or videos that you send to iOS devices and Macs over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles." *Id.* "If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you

According to Mr. Johnson, Ms. Lawn indicated to the police that she "immediately" began texting C.C.'s roommates after Ms. Lawn left Mr. Johnson's bedroom, leaving C.C. in the company of both defendants. Mr. Johnson also alleged that interviews with the police indicated that the police "may have even instructed, advised, or at the very least insinuated to" C.C. and other State's witnesses that they should remove social media information "from public view" and should refrain from communicating about the offenses via social media. Mr. Johnson indicated that he had learned from the State that the police had searched, but had not preserved, any social media communications. He also noted that the police had preserved all the data from Mr. Johnson's cellular telephone but had preserved none from cellular telephones belonging to C.C. or any other State witness.

At the August 24, 2015 hearing on the defendants' motion, counsel for Mr. Johnson indicated that after learning that the Knoxville Police Department ("KPD") had "sent preservation letters under the Electronic Stored Communications Act to communication providers to preserve information from certain witnesses, namely, [C.C.] and Ms. Lawn," the defendants sent a specific discovery request for that information. In its response to the specific discovery motion, the State related that the KPD "did not, in fact, obtain the messaging information of its witnesses." Counsel insisted that the information was necessary to ensure that Mr. Johnson received a fair trial and moved the court to provide an order "that compels, along with the subpoenas that will be issued, the various service providers to provide the . . . data communications" to the trial court under seal.

The State opposed the motion on grounds that the motion, which was filed on the Friday before the first trial was set to begin, was untimely, noting that the State had "incurred a large expense . . . in preparing for this trial" and that several of the State's witnesses had obligations related to their status as student athletes that presented scheduling difficulties. The State also argued that the defendants had failed to allege specific facts to support the issuance of the subpoenas, describing the subpoena request as "nothing more than an 11th-hour fishing expedition." The State observed that the defendants had also failed to identify any particular piece of admissible evidence that would be uncovered.

send to other cell phones or iOS devices. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device." *Id.* "When you send a text message to someone that has an Apple ID, the Messages app automatically recognizes that person's Apple ID and routes the message through Apple's servers instead of using the cell phone carrier. This is done automatically and avoids any texting charges from the cell phone carrier." http://www.ianswerguy.com/imessage-difference/ (last visited February 1, 2017).

The trial court had previously granted Mr. Johnson's motion to sever his trial from that of Mr. Williams.

With regard to timing, counsel for Mr. Johnson stated that the State had provided them with Mr. Johnson's cellular telephone data in the week before trial and that he had only learned two days before filing the motion that the State had not obtained any electronic communications from anyone other than Mr. Johnson. Citing *United States v. Nixon*, 418 U.S. 683 (1974), counsel argued that Mr. Johnson need only "establish that there could be information that's material and relevant on there." He observed that the discovery materials were replete with information that "there was a lot of text messaging and social media communications that were going on about this party that night" and that, Ms. Lawn in particular, participated in social media and text messaging communications immediately after leaving C.C. in Mr. Johnson's bedroom in the company of the defendants. Counsel also pointed to KPD interviews where C.C. and other witnesses discussed with KPD detectives "about whether or not they should have their social media taken down."

The State argued that the defendants had failed to satisfy the *Nixon* standard and argued that the information sought by the defendants qualified as witness statements, which would not be discoverable prior to trial under the terms of Tennessee Rule of Criminal Procedure 26.2. The defendants countered that the information could not be covered by Rule 26.2 because that rule, by its terms, is restricted to information in possession of the parties.

At the conclusion of the hearing, the court granted the motion, stating that it felt "compelled to give the defendant[s] a full opportunity to gain any information that may be helpful to their case." The court ordered that the materials be returned to chambers by September 8, 2015. In the written order, the court found "that specific and articulable facts establish[ed] reasonable grounds to believe that records and information pertaining to designated cellular telephone and social media communications are relevant and material to a pending criminal matter." On that same day, the court entered a protective order that provided that "all materials produced to the court subject to the said Order and subpoenas duces tecum are to be filed under seal and made a part of the technical record in this matter." The protective order also provided for "[e]xact duplicates of all materials . . . to be provided in their entirety to counsel for the parties."

Immediately following the hearing, the defendant issued and served 21 subpoenas duces tecum:

Provider	Information Requested	Persons Covered	Timeframe
AT&T Mobility	"[a]ll stored electronic	C.C.	11/1/2014 -
	communications" "and the	Ms. Lawn	present
	related account records,		

	. 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
	including but not limited to		
	the call detail records		
	(including all incoming and		
	outgoing calls, the duration		
	of said calls, the time and		
	date of said calls, and the cell		
	site addresses and/or cell		
	tower information associated		
	with said calls), audio		
	recordings, saved contacts,		
	geolocation data, text		
	messages or iMessages sent		
	or received, photographs,		
	video recordings, and		
	voicemail messages"		
Instagram <sup>5</sup>	"[a]ll stored electronic	C.C.	1/1/2014 -
	communications" including	Ms. Lawn	present
	"basic subscriber information	Ms. Boland	
	(including Instagram	Ms. Tavares	
	username, e-mail address,		
	telephone number, and		
	timestamps and IP addresses		
	for account logins/logouts),		
	photographs, photo captions,		
	and other posts from the		
	subscriber's Instagram		
	accounts(s), and the content		
	of messages, photos,		
	comments, and location		
	information"		
Twitter <sup>6</sup>	"[a]ll stored electronic	C.C.	1/1/2014 -

<sup>&</sup>lt;sup>5</sup> "Instagram is a social networking app made for sharing photos and videos from a smartphone." "It's like a simplified version of Facebook, with an emphasis on mobile use and visual sharing. Just like other social networks, you can interact with other users on Instagram by following them, being followed by them, commenting, liking, tagging and private messaging." https://www.lifewire.com/what-is-instagram-3486316 (last visited February 8, 2017).

<sup>&</sup>lt;sup>6</sup> "Twitter is a free micro-blogging tool that allows users to publish short messages (140 characters or less) through their computers and mobile phones." "People who use Twitter write short messages, called Tweets, which they publish either publicly (for all Twitterers to see) or privately (for only certain Twitterers to see)." https://www.lifewire.com/twitter-basics-3476455 (last visited February 8, 2017).

	communications" including "account/user information (including username(s)), the associated 'Twitter archive,' communications and/or content (including following, followed, muted, and blocked accounts, status updates ('tweets') posted and replies received, 'tweets' marked as a 'favorite,' direct messages sent and received, list memberships, lists subscribed to, and uploaded files (including photographs and video files and whether through pic.twitter.com, Periscope, Vine, or any other means)), and geolocation data"	Ms. Lawn Ms. Boland Ms. Tavares	present
Snapchat <sup>7</sup>	"[a]ll stored electronic communications" including "basic subscriber information (including Snapchat username, e-mail address, telephone number, and timestamps and IP addresses for account logins/logouts), logs (including sender, recipient, date, and time) of 'snaps,' 'stories,' and/or 'chats' sent to or from the subscriber's Snapchat account(s), and the content of 'snaps,' 'stories,' and/or 'chats' sent to or from the	C.C. Ms. Lawn Ms. Boland Ms. Tavares	1/1/2014 – present

<sup>&</sup>lt;sup>7</sup> "Snapchat is both a messaging platform and a social network" that "exists only as a mobile app you can download to your iPhone or Android smartphone." Snapchat "[p]hotos and videos essentially disappear a few seconds after they've been viewed by their recipients" unlike "other social networks, which keep your content online forever unless you decide to delete it." https://www.lifewire.com/whatis-snapchat-3485908 (last visited February 8, 2017).

	subscriber's Snapchat		
	account(s)"		
Facebook	"[a]ll stored electronic	C.C.	1/1/2014 -
	communications" including	Ms. Lawn	present
	"basic account/user	Ms. Boland	
	information (including user	Ms. Tavares	
	identification number(s)		
	and/or username(s), e-mail		
	address(es), registered mobile		
	telephone number, etc.),		
	expanded subscriber content		
	(including profile contact		
	information, status update		
	history, shares, notes, wall		
	postings, list of 'friends and		
	other accounts 'followed,'		
	list of 'pages' 'liked,' list of		
	groups joined, future and past		
	events, video files, etc.), user		
	photos (whether uploaded by		
	the user or by other users),		
	private messages sent and		
	received, activity logs, and		
0	geolocation data"		
Yik Yak, Inc. 8	"[a]ll stored electronic	C.C.	1/1/2014 -
	communications" including	Ms. Lawn	present
	"each message posted, the IP	Ms. Boland	
	address from which each	Ms. Tavares	
	message was posted, the		
	Global Positioning System		
	('GPS') coordinates of the		
	location from which each		
	message was posted, the time		
	and date when each message		
	was posted, and the user-		
	agent string associated with		
	the device from which each		

<sup>8 &</sup>quot;Yik Yak is basically an anonymous location-based status posting app for your local community, which shows you anonymous posts from people around your geographical area." https://www.lifewire.com/what-is-yik-yak-3485928 (last visited February 2, 2017).

On September 11, 2015, Mr. Johnson filed a motion asking the trial court "to set a date certain for the pretrial inspection of specified cellular telephone and social media communications and information sufficiently in advance of trial to permit the parties' meaningful inspection and analysis" of the materials and "to issue the necessary process to secure the attendance at the pretrial inspection of the out-of-state witnesses with custody of said communications and information." In support of his motion, counsel for Mr. Johnson indicated that they were "actively working" to obtain the requested materials from Yik Yak, which counsel deemed "likely to comply" with the subpoena. Additionally, counsel averred that AT&T had marked the subpoena as "urgent" to assure quick compliance. Counsel averred that Facebook, Instagram, Snapchat, and Twitter had "responded to the Court's Order and subpoenas with objections" in the form of a letter sent to defense counsel. Those providers "recommended" that the defendants "obtain the subpoenaed communications and information directly from the" account holders.

Without accepting the validity of the service providers' objections, Mr. Johnson informed the court of his intention to issue additional subpoenas duces tecum to the four individual account holders requesting "the same communications and information previously subpoenaed from their service providers." To facilitate this process for the three witnesses who were, at that time, residing out of state, Mr. Johnson moved the court to issue the necessary process to secure the attendance of each witness at the pretrial inspection of the materials.

Three days later, on September 14, 2015, Mr. Johnson moved the trial court to hold Facebook, Instagram, Snapchat, and Twitter in contempt for failing to comply with the court's order and subpoenas. Mr. Johnson noted that although those service providers had objected to the subpoenas via letter, none had filed a motion to quash. On the following day, Mr. Johnson moved the court "to compel the state to request search warrants to obtain the specified social media communications and information previously subpoenaed pursuant to the Court's Order of August 24, 2015." Mr. Johnson claimed that responses from Facebook, Instagram, Snapchat, and Twitter indicated that those providers would release the subpoenaed information pursuant to a search warrant. Mr. Johnson also moved the court on September 15, 2015, "to issue the necessary process [to] secure the compliance of out-of-state service providers with the Court's previous Order and accompanying Subpoenas Duces Tecum regarding specific social media communications" and "to reset the date for compliance with the same to September 28, 2015." In a supplemental motion also filed on September 15, 2015, Mr. Johnson

<sup>&</sup>lt;sup>9</sup> C.C., Ms. Boland, and Ms. Lawn.

informed the court that counsel for Facebook, Instagram, and Twitter had informed counsel for Mr. Johnson that those entities planned to secure local counsel to file responsive pleadings and "to address the multiple matters of first impression presented in this case surrounding the [F]ederal Stored Communications Act." Mr. Johnson also noted that counsel for those providers indicated during a telephone conversation "that some of the communications at issue are no longer available possibly due to deletion by the content subscriber."

Following a hearing on September 17, 2015, the trial court held in abeyance the motion to hold the service providers in contempt. The court also modified the time for compliance with the subpoenas to September 28, 2015. Also on that date, the defendants issued subpoenas to the four witnesses that required production of each witness' current and former cellular telephone handsets and copies "in native format" of all the data "associated with any and all" current and former Facebook, Instagram, Twitter, Snapchat, and Yik Yak accounts for the period between May 15, 2014, and December 31, 2014. Each subpoena contained directions for obtaining the necessary information from Facebook, Instagram, Twitter, and Snapchat. None explained how the data could be retrieved from Yik Yak. The trial court issued certificates of materiality to accompany the subpoenas.

On September 28, 2015, the State moved to quash the subpoenas issued to C.C., Ms. Boland, Ms. Lawn, and Ms. Tavares, claiming that "[c]ompliance with these [s]ubpoenas is unreasonable and oppressive" and that "the [s]ubpoenas are cumulative in that they seek information and records that are already being sought by subpoenas issued to various communications/social media providers." In its motion, the State averred that "[i]n some instances, the witnesses never had social media accounts with the companies listed in the [s]ubpoenas," that "[i]n some instances, the witnesses have found it impossible to limit data retrieval to the time period listed in the [s]ubpoenas," and that "the [a]ttachment to the [s]ubpoenas provides no instructions at all for retrieving data from Snapchat or Yik Yak." The State attached to its motion an email from Ms. Boland's mother that it claimed "detail[ed] the onerous nature of the data-retrieval portion of the [s]ubpoenas." The State also noted that the attachment to the subpoenas issued to the four witnesses contained a requirement that the witnesses "provide for inspection any cellular telephone handset that they used primarily or exclusively between May 15, 2014 through December 31, 2014" when the trial court's order did not cover these cellular telephone handsets.

Also on September 28, 2015, the State moved the trial court "to modify all subpoenas issued concerning the communications/social media accounts of" C.C., Ms. Lawn, Ms. Boland, and Ms. Tavares, arguing that "the time frame for most of the subpoenaed materials is overly broad." The State asked that the subpoenas issued to the

social media service providers regarding C.C.'s accounts be modified to cover communications between May 15, 2014, and December 31, 2014. The State asked that the subpoenas issued to the social media service providers regarding the remaining witnesses' accounts be modified to cover communications from November 15, 2014, to December 31, 2014. In support of its request, the State posited that there had "been no showing that social media or telephonic activity concerning the event in question actually occurred before the offense."

On October 20, 2015, Mr. Johnson moved the trial court to compel the four witnesses to show cause as to why they should not be held in contempt for failing to comply with the subpoenas. Mr. Johnson indicated that he had sent the subpoenas to the three out-of-state witnesses on September 21, 2015, "by FedEx priority overnight service with adult signature required." C.C. and Ms. Boland received and signed for the packages on the following day. C.C. was served with domesticated Florida process on September 24, 2015. Delivery to Ms. Lawn was attempted on "three consecutive days until September 24, 2015, when someone requested that the package be held at the local FedEx facility." After three more days passed without anyone retrieving the package, it was returned to counsel for Mr. Johnson. Mr. Johnson then sent a second package to Ms. Lawn without a signature requirement, and that package was delivered on September 29, 2015.

According to Mr. Johnson, on September 22, 2015, C.C. sent a letter along with "an assortment of printouts from various social media service providers" to the trial court. This assortment did not include any electronic communications made during the week surrounding the alleged offenses in this case. It did include printouts from Instagram, Twitter, and Snapchat that appeared to explain why she had been unable to retrieve the subpoenaed information. The letter, which was filed under seal but appended to Mr. Johnson's motion, does support Mr. Johnson's statement that C.C. upgraded to a new cellular telephone handset on January 27, 2015. She claimed that the older handset had malfunctioned but stated that she had sold the telephone through a website after restoring it to the default factory settings. As of October 20, 2015, none of the remaining witnesses had returned any of the subpoenaed materials to the court. Mr. Johnson asked that the witnesses be made to show cause for their failure to comply and that the court enforce the statutory forfeiture for their noncompliance.

Mr. Johnson also stated that the responsive documents received from AT&T indicated that both C.C. and Ms. Lawn had disposed of their cellular telephone handsets "within 24 hours of one another on January 27 and 28, 2015." In the letter, which was appended to the pleading, AT&T indicated that it had not stored the content of text messages for either C.C. or Ms. Lawn but that iMessages might be retrieved from

either witness's iCloud<sup>10</sup> account. AT&T also stated that it could not provide access to voicemail within a certain timeframe; that, generally, it retained voicemails only for 14 to 30 days; and that voicemails deleted by the customer could not be recovered at all. Mr. Johnson moved the court to require both C.C. and Ms. Lawn to provide their iCloud login credentials to Sword & Shield Enterprise Security, Inc., "to download the witnesses' data, limit the data retrieved to the time periods stated in the [s]ubpoenas, and provide the responsive data to the Court and all counsel."

On October 20, 2015, local counsel for Facebook, Instagram, Snapchat, and Twitter (hereinafter collectively "the social media providers")<sup>11</sup> filed a "Notice" of the status of the subpoenas issued to those parties. In the notice, the social media providers indicated that the subpoenas issued to all but Snapchat had been domesticated in California but nevertheless maintained that the Stored Communications Act ("SCA") did not authorize them to release the contents of electronic communications to criminal defendants. The social media providers contended that the appropriate procedure was to subpoena the information directly from the users. Twitter, in particular, "confirmed and advised" local counsel "that it has no records to produce in response to any" of the subpoenas. Facebook and Instagram agreed "to produce non-content records . . . as permitted under the SCA, after giving the users 21 days' notice and an opportunity to object." The social media providers did not take any position regarding the State's motion to quash but did "reserve any and all objections that may be asserted to the subpoenas." The social media providers also noted that "any objections that cannot be consensually resolved" would be "properly litigated in the California court from which the [s]ubpoenas issued." The notice also indicated that counsel for Mr. Johnson had agreed to stay compliance with the subpoenas and to withdraw his motion for contempt. 12

On October 23, 2015, Mr. Johnson moved the court to dismiss the presentment, exclude the testimony of the witnesses, or issue an adverse inference instruction based upon the State's failure to preserve the electronic communications that were the subject of the subpoenas. He argued that because the police were aware that several of the witnesses in this case used text messaging and social media to communicate before and after the alleged offenses, they should have endeavored to

<sup>10 &</sup>quot;At its most basic level, 'the cloud' is the Internet, or more accurately, a piece of the Internet." https://www.lifewire.com/what-is-icloud-3972867 (last visited on February 3, 2017). "The 'iCloud' is the generic name for . . . . Apple's 'cloud-based' or Internet-based services." *Id.* The "iCloud automatically backs up the information" stored on Apple "devices—iPhone, iPad, and iPod touch—over Wi-Fi every day when they are turned on, locked, and connected to a power source." This daily backup covers "iMessage, text (SMS), and MMS messages." https://support.apple.com/kb/ph12519?locale=en\_US (last visited on February 3, 2017).

<sup>11</sup> Yik Yak has not objected to the subpoenas at any point.

<sup>&</sup>lt;sup>12</sup> Mr. Johnson, in other pleadings, indicates that the motion for contempt was held in abeyance rather than withdrawn.

preserve those communications. Mr. Johnson also noted that, following the alleged offenses, C.C. gave conflicting statements and that, following her interviews with KPD detectives, she had reset her cellular telephone to its factory settings, thereby deleting her text messages and contact information. Although she claimed that she disposed of the cellular telephone because it no longer worked, she stated that she sold the device on a website. She also deleted her Twitter and Instagram accounts and deactivated her Facebook account. Ms. Lawn similarly disposed of her cellular telephone. In that same pleading, Mr. Johnson indicated that he would not contest the State's motion to modify the timeframe of the subpoena.

On October 27, 2015, the State filed an amended motion to quash. In its amended motion, the State challenged the subpoenas issued to AT&T, the social media providers (including Yik Yak), and the four witnesses. The State argued that the defendants had failed to show that the subpoenas will produce material evidence and that compliance with the subpoenas was unreasonable and oppressive. The State asserted that the subpoena to C.C. violated her rights as a victim. Finally, the State claimed that granting subpoenas would have a chilling effect on rape reporting.

In his response to the State's amended motion to quash, Mr. Johnson argued that the court had already determined, following a contested hearing, that the information covered by the subpoenas was both relevant and material. He stated that the information already disclosed pursuant to the subpoenas confirmed the court's finding. Mr. Johnson also claimed that the State lacked standing to challenge the subpoenas because the State had no "personal right, privilege, or proprietary interest" in the subpoenaed materials. Finally, Mr. Johnson argued that, even if the State had standing to challenge the subpoenas, it could not establish that the subpoenas were unreasonable or oppressive.

Neither party presented evidence at the November 3, 2015 hearing on the motion to quash. The State argued that the defendants had made "no showing that these subpoenas will lead to material and admissible evidence," explaining that materiality was "the main reason that we're here in court today." The State claimed that the defendants had failed to make even a showing that each of the witnesses had accounts with each of the social media providers. The State insisted that the defendants could obtain text messages exchanged between them and any of the witnesses from the defendants' cellular telephones. The State asserted that the defendants had presented no proof of the need to confiscate the cellular telephones of C.C. and Ms. Lawn. The State emphasized that the "main issue" as far as the State was concerned was "that these subpoenas are unsupported by material or admissible evidence." The State also argued, however, that "these subpoenas are oppressive and unreasonable, under Rule 17," citing as proof the email sent to the prosecutor by Ms. Boland's mother as exhibited to their motion to quash, in

which Ms. Boland's mother claimed that she and her husband had spent several hours attempting to assist Ms. Boland in complying with the subpoena and that compliance had been more time consuming than anticipated, to support its assertion that compliance with the subpoenas was unreasonable. Finally, the State asserted, as it had in its amended motion to quash, that requiring C.C. to comply with the subpoenas would create a chilling effect on rape reporting and prosecuting.

The defendants argued that the State had failed to establish any need for the court to revisit its earlier ruling that the subpoenaed materials were material and relevant. The defendants also asserted that the State's motion to quash was untimely because some of the witnesses and some of the providers had already begun to comply with the subpoenas. Finally, the defendants maintained that the subpoenas were not unreasonable or oppressive and that there was no practical or legal reason to stop the subpoena process after compliance had begun and so close to trial. The defendants suggested that if the witnesses were experiencing technical difficulties, then the court should appoint an expert to help them at the defendants' expense.

At the conclusion of the hearing, the trial court granted the motion to quash as to the four witnesses and denied the motion as to all the service providers, ruling as follows:

As we said over and over, we're plowing new ground here. This is new territory. We're faced with the reality of the computer age and the generation of incredible amounts of communication and the ability to store these communications and access them. It is a new world and there's much more information available now than there has been in the past.

And the way that legal principles concerning the acquisition of information in litigation is — is struggling to keep up. We are not — our legal processes have not fully embraced and resolved the manner in which this immense amount of information is to be shared, distributed. So we are without a great deal of guidance and authority in making these decisions and in managing this case.

In the beginning, this started with the defense argument – which the Court accepted. The Court accepted defense counsel's representations that Federal case law and Federal statutes are advancing the proposition that stored media communication should be made available to defendants

in criminal prosecutions. That's how all of this started. The Court accepted that proposition. The Court reviewed 18 United States Code Annotated, 2701 et seq. And this is the Stored Wire and Electronic Communications and Transactional Records and Access Act. And that's how we began this journey into the business of computer recorded and stored communication information.

In . . . accord with that finding, and with that proposition, this Court did approve the subpoena duces tecum and the accompanying orders to cause social media service providers to provide to the Court the social media communication information relevant to this case. That was the next step.

Some information was provided to the Court pursuant to the subpoenas from some of the providers. Other servers reported that it was their policy to leave it to the end users, or customers, to provide the communication information to others.

In response, counsel for the defense sought approval by this Court for subpoenas and orders directed to the end users, or customers, identified in this case as [C.C.], Bridget Boland, Anna Lawn and Natalie Tavares.

At this point, it appeared to the Court that there was some consensus between the State and the defense that it was appropriate for the end users, or customers, to provide this information to the Court. There was some agreement that the State's attorneys would attempt to help these end users provide this information.

In the attempt to do so, however, it became apparent that the end users, or customers, were not able to access the information in spite of what appeared to be sincere efforts to do so.

At this point, the State filed the motion to quash the subpoena. Under these circumstances, this Court finds that those circumstances justify the extension of the time allowable to the State to file its motion. There w[ere] circumstances that developed after – during the attempt to comply with the subpoena that the State learned that this, in their view, was oppressive and the subpoena should be quashed.

At this point today, this morning . . . the defense is asking the Court to enforce the subpoenas and the State is asking the Court to quash the subpoenas.

It now falls to this Court, in this case, to try to find the proper response of a State trial court to evolving Federal law pertaining to access for both the prosecution and the defense to the expediential increase of stored social media communication information available today.

First, this Court is going to distinguish between two types of social media communication information. The first type the Court will refer to as structural information. By this, the Court means the existence of communications, their duration, the identities of the end users, or customers, who are sending or receiving the communications and, where possible, the location of the senders and receivers. Other types of information might also be considered as structure.

The second type of social media communication information this Court will recognize is content.

The Court now considers the four subpoenas on the individuals, [C.C.], Ms. Boland, Ms. Lawn and Ms. Tavares. First of all, the Court does find that the State has standing to move to quash subpoenas that are being used to try to seize information from their witnesses or potential witnesses.

In considering the relationship between Tennessee law and the Federal statutes and case law pertaining to subpoenas, this Court finds as follows:

Part A. In the context of this case, the term "content," . . . is equivalent to the legal phrase "statements of witnesses."

Tennessee Rule of Procedure, Rule 17, clearly excludes statements of witnesses from the subpoena power. The Federal statute deals only with the production of information by service providers and not by end users, or customers. That's the second part.

The third part – the third finding of the Court is: That this Court does find that the subpoenas on the individuals in this case are oppressive and unreasonably demanding. The contention made by the State – rather by the defense, that the Court should appoint a computer expert to assist compliance with the subpoena only underscores the unreasonableness of the subpoena obligation as to those private end users.

And for those three reasons, the fact that Tennessee Rule of Procedure, Rule 17, excludes statements of witnesses, and the Federal law deals only with the service providers and not the end users, and in this case, certainly, the Court is finding that the subpoenas turn out to be oppressive and unreasonably demanding. For these three reasons, the Court does now grant the State's motion to quash the subpoenas that have been issued to [C.C.], Bridget Boland, Anna Lawn and Natalie Tayares.

The Court does find that the State lacks standing to move to quash the subpoenas that were issued to the service providers themselves.

In response to questions by the defense, the court stated that the subpoenas issued to the service providers "remain intact," explaining, "Those people truly are third . . . parties to this litigation. And they're all perfectly capable of hiring lawyers and moving to quash if they choose to." The court specifically did not rule on whether the providers had to provide the content of the communications.

Following the trial court's November 3, 2015 order, both parties moved the trial court for permission to seek interlocutory appeal. The trial court granted permission, and this court agreed to interlocutory review, framing the scope of review as follows:

To be clear, this interlocutory review concerns only the trial court's November 3, 2015 order granting, in part, and denying, in part, the State's motion to quash subpoenas of the

alleged victim, witnesses, and social media service providers, as limited by the trial court's November 3 order and order granting permission to seek interlocutory appeal.

Thus, we review the trial court's conclusion that the State had standing to quash the subpoenas duces tecum issued to the witnesses, the court's ruling quashing those subpoenas, and the court's ruling that the State did not have standing to quash the subpoenas duces tecum issued to the various service providers.

## I. Standing

The defendants argue that the State lacks standing to file a motion to quash any of the subpoenas issued in this case because the State lacks "a personal right, privilege, or proprietary interest" in the materials the defendants seek via the subpoenas. The State asserts that it has standing based upon its legitimate interests in preventing an unnecessary delay of the trial and protecting the State's witnesses. The State also contends that because it bears a constitutional and statutory "duty to protect the rights of crime victims and prosecution witnesses alike," it has standing to contest subpoenas that "threaten" the rights or interests of the victim and the State's witnesses.

As the defendants correctly observe, the trial court did not apply the test for standing to challenge a third party subpoena adopted in *State v. Harrison*, 270 S.W.3d 21 (Tenn. 2008), and instead concluded, without any analysis, "that the State has standing to move to quash subpoenas that are being used to try to seize information from their witnesses or potential witnesses." Similarly, the court found, in conclusory fashion, "that the State lacks standing to move to quash the subpoenas that were issued to the service providers themselves." In response to a question from defense counsel, the court clarified that the service providers "truly are third . . . parties to this litigation. And they're all perfectly capable of hiring lawyers and moving to quash if they choose to."

The subpoenas in this case were issued pursuant to Rule 17 of the Tennessee Rules of Criminal Procedure, which rule provides that "[a] subpoena may order a person to produce the books, papers, documents, or other objects the subpoena designates" either "in court before trial or before they are to be offered in evidence." Tenn. R. Crim. P. 17(d)(1). "On motion made promptly and in any event by the time specified in the subpoena for compliance therewith, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive." Tenn. R. Crim. P. 17(d)(2). The rule is silent on the issue of who may move to quash a subpoena.

Absent a showing that the State had standing to challenge the subpoenas, the controversy is not justiciable. West v. Schofield, 468 S.W.3d 482, 490 (Tenn. 2015)

("To determine whether a particular case involves a legal controversy, Tennessee courts use justiciability doctrines that 'mirror the justiciability doctrines employed by the United States Supreme Court and the federal courts,' and these doctrines 'include: (1) the prohibition against advisory opinions, (2) standing, (3) ripeness, (4) mootness, (5) the political question doctrine, and (6) exhaustion of administrative remedies." (citations omitted)); City of Memphis v. Hargett, 414 S.W.3d 88, 96 (Tenn. 2013) ("Justiciability encompasses several distinct doctrines, two of which are . . . mootness and standing."). As the moving party, the State bore the burden of establishing its standing to challenge the subpoenas in this case. ACLU of Tenn. v. Darnell, 195 S.W.3d 612, 620 (Tenn. 2006). Because standing presents a question of law, we review the issue de novo with no presumption of correctness afforded to the trial court. Massengale v. City of East Ridge, 399 S.W.3d 118, 123 (Tenn. Ct. App. 2012) (citing Cox v. Shell Oil Co., 196 S.W.3d 747, 758 (Tenn. Ct. App. 2005)).

Standing, "a judge-made doctrine," Fannon v. City of LaFollette, 329 S.W.3d 418, 424 (Tenn. 2010) (quoting Knierim v. Leatherwood, 542 S.W.2d 806, 808 (Tenn. 1976)), is designed "to determine whether a particular litigant is entitled to have a court decide the merits of a dispute or of particular issues," Darnell, 195 S.W.3d at 619. "Grounded upon 'concern about the proper—and properly limited—role of the courts in a democratic society,' the doctrine of standing precludes courts from adjudicating 'an action at the instance of one whose rights have not been invaded or infringed." Id. (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975); Mayhew v. Wilder, 46 S.W.3d 760, 767 (Tenn. Ct. App. 2001)). "Every standing inquiry requires a 'careful judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted." Hargett, 414 S.W.3d at 97 (quoting Allen v. Wright, 468 U.S. 737, 752 (1984)).

In *Harrison*, the supreme court considered whether Harrison had standing to challenge a subpoena directing Dr. Dennis Wilson, a clinical psychologist who had conducted a forensic examination of Harrison, "to produce '[a]ny and all records' retained by him related to his psychological evaluation." *State v. Harrison*, 270 S.W.3d 21, 26 (Tenn. 2008). Although the *Harrison* court was examining a judicial subpoena issued under the terms of Code section 40-17-123, which prescribes the procedure to "be employed when a law enforcement officer, as defined in § 39-11-106," requests "the production of books, papers, records, documents, tangible things, or information and data electronically stored for the purpose of establishing, investigating or gathering evidence for the prosecution of a criminal offense," T.C.A. § 40-17-123(a), we see no reason that the court's analysis is inapplicable to subpoenas issued pursuant to Rule 17.

In keeping with the general rule reached by numerous courts that "[a] party has standing to move to quash a subpoena addressed to another if the subpoena infringes

upon the movant's legitimate interests," *see United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982), our supreme court concluded that "[a] person who does not have a legally protectable interest in subpoenaed materials has no standing to challenge either the form of a subpoena issued to a third party or the manner in which the subpoena was issued," *see Harrison*, 270 S.W.3d at 28. In consequence, the court held that only "a person who has a personal right, privilege, or proprietary interest in materials subject to a third-party subpoena has standing to challenge the subpoena." *Harrison*, 270 S.W.3d at 28-29. Accordingly, the court held that Harrison had standing to challenge the subpoena.

Citing *Ranieri*, the State argues that it has a legally protectable interest in the subpoenas arising from its "interests in preventing undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [witness] credibility." *See Raineri*, 670 F.2d at 712. The State also asserts that it has standing to advocate the four witnesses' personal rights to the subpoenaed materials by virtue of its statutory and constitutional duty to protect the privacy rights of the victims and witnesses of crime. We consider each claim in turn.

### A. The State's Own Interest

The State, because of its unique position as "the representative not of an ordinary party to a controversy" but of the people of the State of Tennessee, *see Berger v. United States*, 295 U.S. 78, 88 (1935), will often lack standing in a criminal case "to challenge a subpoena issued to a third party because of the absence of a claim of privilege, or the absence of a proprietary interest in the subpoenaed material or of some other interest in the subpoenaed documents," *United States v. Beckford*, 964 F. Supp. 1010, 1023 (E.D. Va. 1997). That is the case here. The State has no personal right, privilege, or proprietary interest *in the electronic communications at issue*. That being said, courts have recognized that the State does have legitimate interests that may, under certain circumstances, provide it with standing to challenge a third party subpoena issued by a criminal defendant. The legitimate State interests most often cited come from *Ranieri*: "preventing undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [witness] credibility." *See Raineri*, 670 F.2d at 712.

In *Ranieri*, the Seventh Circuit Court of Appeals concluded that the government had standing to challenge a subpoena issued by Ranieri to a government witness during trial. The prosecution presented out-of-state witness Cira Gasbarri as its first witness during Ranieri's trial on charges that he ran a prostitution ring. The defendant subjected her to two days' cross-examination. *Id.* Nearly three weeks later, Ranieri issued an ex parte subpoena for Gasbarri to appear as a defense witness. *Id.* The prosecution successfully moved to quash the subpoena. The court stated, without analysis, discussion, or citation to any authority, that "[t]he prosecution's standing rested

upon its interest in preventing undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on Gasbarri's credibility." *Id.* A number of state and federal courts have applied the holding in *Ranieri* to the determination whether the prosecution in a criminal case has standing to challenge a subpoena issued by the defendant to a third party. *See, e.g., United States v. Segal*, 276 F. Supp. 2d 896, 900 (N.D. Ill. 2003); *United States v. Daniels*, 95 F. Supp. 2d 1160, 1164 (D. Kan. 2000); *United States v. Nachamie*, 91 F. Supp. 2d 552, 558 (S.D.N.Y. 2000); *Schreibvogel v. State*, 228 P.3d 874, 880 (Wyo. 2010); *Com. v. Lam*, 827 N.E.2d 209, 214 (Mass. 2005); *State v. DeCaro*, 745 A.2d 800, 816 (2000).

Because Harrison involved the defendant's challenge to a third party subpoena, our supreme court had no occasion to determine when the State would have standing to challenge a third party subpoena. Thus, Harrison's holding is expressed in terms of what "a person" must show to establish standing: "a personal right, privilege, or proprietary interest." As indicated above, it will be difficult if not impossible for the State in a criminal case to establish specifically "a personal right, privilege, or proprietary interest." The Harrison court made it clear, however, that its holding was grounded in the conclusion that "[a] person who does not have a legally protectable interest in subpoenaed materials has no standing to challenge either the form of a subpoena issued to a third party or the manner in which the subpoena was issued." Harrison, 270 S.W.3d at 28 (emphasis added). That the high court cited *Ranieri* in support of that conclusion suggests that "a legally protectable interest," as applied to the State in a criminal case, may extend beyond the concepts of "personal right, privilege, or proprietary interest" to cover the State's legitimate interests in "preventing undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [witness] credibility," as described in Ranieri. Id. at 29; Ranieri, 670 F.2d at 712.

In our view, none of the interests identified in *Ranieri* are implicated by the third party subpoenas issued in this case.

First, because the subpoenas were issued prior to trial, there is no danger of undue lengthening of *the trial*. "To the contrary, a subpoena returnable before trial will avoid delay in the government's prosecution of the case." *United States v. Tomison*, 969 F. Supp. 587, 596 (E.D. Cal. 1997) (citing *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951)). The Supreme Court has observed that the "chief innovation" of Rule 17 was, in fact, "to expedite the trial by providing a time and place before trial for the inspection of the subpoenaed materials." *See Bowman Dairy Co.*, 341 U.S. at 220. The record indicates that the defendants sought the subpoenas for the service providers as soon as it became clear that the desired information would not be produced during the discovery process. Then, when the service providers indicated that the defendants should seek the information from the end users, the defendants asked for subpoenas to be issued

to the witnesses. In short, the record gives no indication that the defendants acted with anything other than urgency in acquiring the subpoenas at issue. In *Ranieri*, "the Government's legitimate interest . . . involved preventing a redundant and time-consuming reexamination of a witness who had already been subjected to a lengthy and effective cross-examination." *Nachamie*, 91 F. Supp. 2d at 559. No such concerns exist here.

Second, nothing in the record suggests that the subpoenas issued to the witnesses in this case caused "undue harassment" of the witnesses or that any of the witnesses, including C.C., was in a particularly vulnerable position. Asking a witness to provide his or her evidence to the court in compliance with a validly issued subpoena, standing alone, cannot qualify as "undue harassment." In our adversarial system of justice, "[t]he need to develop all relevant facts . . . is both fundamental and comprehensive." United States v. Nixon, 418 U.S. 683, 709 (1974). To this end, "it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." Consequently, it is "a fundamental maxim that the public . . . has a right to every man's evidence." United States v. Bryan, 339 U.S. 323, 332 (1950). "The defendant's right to compulsory process is itself designed to vindicate the principle that the 'ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." Taylor v. Illinois, 484 U.S. 400, 411-12 (1988) (quoting Nixon, 418 U.S. at 709); see also Nixon, 418 U.S. at 711 ("The right to the production of all evidence at a criminal trial similarly has constitutional dimensions."). To be sure, complying with the subpoenas in this case will require some sacrifice on the part of the witnesses, but "[t]he personal sacrifice involved is a part of the necessary contribution of the individual to the welfare of the public." Blair v. United States, 250 U.S. 273, 282 (1919); see also Blackmer v. United States, 284 U.S. 421, 438 (1932) ("It is also beyond controversy that one of the duties which the citizen owes to his government is to support the administration of justice by attending its courts and giving his testimony whenever he is properly summoned.").

Although the State argues otherwise, there has been no showing that any of the witnesses are "peculiarly vulnerable." Other courts have concluded that the prosecution has standing to challenge a subpoena issued to a "peculiarly" or "particularly" vulnerable witness such as the minor victim of a sexual assault, see Com. v. Lam, 27 N.E.2d 209, 214 (2005) (subpoena issued to the father of the minor victim); People v. Spykstra, 234 P.3d 662, 667 (Colo. 2010) (subpoena issued to the parents of the minor victim), or witnesses in a case where there exists a real potential for violence or threats of violence to the witnesses, see United States v. Orena, 883 F. Supp. 849, 853 (E.D.N.Y. 1995) (subpoena issued to the cooperating witnesses in the witness protection program and their families in a case where the defendants were "alleged to be aligned

with the Orena faction of the Colombo Organized Crime family" in a plot "to murder members of the Persico faction" of the same crime family); United States v. Joseph Anthony Giampa, a/k/a "Joey G.," a/k/a "Big Joe," and Santo Giampapa, Jr., a/k/a "Jay," a/k/a "Jay G.," a/k/a "Jr.,", No. S 92 CR. 437 (PKL), 1992 WL 296440, at \*1 (S.D.N.Y. Oct. 7, 1992) (subpoenas issued to cooperating witness, his wife, and minor son, all of whom were in the witness protection program, by defendants "charged with the murder of Michael Salerno, conspiracy to murder Mr. Salerno, and conspiracy to assault Warren Ulrich in aid of a racketeering enterprise known as the Luchese Organized Crime Family of La Cosa Nostra"). Instead, the witnesses here are adults with no demonstrated vulnerabilities that would give rise to the State's standing to challenge the subpoenas as a means of protection. That they have been identified as potential witnesses by the State could not be sufficient, in and of itself, to provide the State with standing. As the Nachamie court recognized, if the State "had standing to move to quash whenever a subpoena was served on a potential witness, then it could move to quash virtually every Rule 17(c) subpoena merely by claiming that the recipient might become a witness." Nachamie, 91 F. Supp. 2d at 560. We agree with that court that, "[s]urely, the concept of standing," a concept that goes to the very jurisdiction of the court, "was not meant to be so elastic." Id.

That the defendants moved the court to hold the witnesses in contempt for failure to comply with the subpoenas does not alter our analysis. The State implies, without any evidence, that the motion for contempt was designed to harass, intimidate, or retaliate against the witnesses. As indicated, "there is a general duty to give what [evidence] one is capable of giving," see Bryan, 339 U.S. at 332, and the appropriate recourse when a party fails to comply with a subpoena, absent some showing of an adequate excuse for failure to comply, is a motion for contempt, see Tenn. R. Crim. P. 17(g) ("When a subpoena is served on a person, the court issuing the subpoena may deem the person's refusal to obey the subpoena to be contempt of court unless the person has an adequate excuse."); see, e.g., Blair, 250 U.S. at 282. We cannot characterize the defendants' attempt to pursue the only remedy available to them as "threatening." "A subpoena has never been treated as an invitation to a game of hare and hounds, in which the witness must [provide evidence] only if cornered at the end of the chase." Bryan, 339 U.S. at 331.

Finally, there is no evidence to suggest that the subpoenas in this case will lead to "a prejudicial over-emphasis on [witness] credibility." Indeed, in a case such as this, in which the determination of the defendants' guilt or innocence will depend solely on the credibility of the witnesses, we cannot fathom that the credibility of the State's witnesses could be overemphasized. That being said, because the subpoenas were issued prior to the trial, issues of credibility of the witnesses or the emphasis thereon are not ripe for our review.

Aside from the three interests mentioned in *Ranieri*, the State will have standing to challenge a subpoena issued to a third party when compliance with the subpoena is "unreasonable or oppressive" *as applied to the State. See, e.g., United States v. Daniels*, 95 F. Supp. 2d 1160, 1164 (D. Kan. 2000); *Tomison*, 969 F. Supp. 587, 596 (E.D. Cal. 1997). Nothing in this case, however, suggests that compliance with the subpoenas will work any particular hardship on the State or indicates that the materials subpoenaed include any work product of the State that might give rise to a proprietary interest in the materials. *See Nachamie*, 91 F. Supp. 2d at 560 (observing that prosecution would have standing to challenge subpoena that requested prosecution work product).

## B. The State as Proxy for the Witnesses' Interests

The State also asserts that its statutory and constitutional duty "to protect the interests of victims and witnesses" in criminal cases creates in the State a legal interest giving rise to standing to challenge the subpoenas in this case. In support of its position, the State points to the supreme court's statement in *Harrison* that a legal right or interest in subpoenaed materials "may, but not must, be created or defined by statute." *Harrison*, 270 S.W.3d at 27. "[I]n cases where a party is seeking to vindicate a statutory right of interest, the doctrine of standing requires the party to demonstrate that its claim falls within the zone of interests protected or regulated by the statute in question." *Id.* at 28 (quoting *Wood v. Metro. Gov't of Nashville & Davidson Cnty.*, 196 S.W.3d 152, 158 (Tenn. Ct. App. 2005)).

The State notes that article one, section 35 of our state constitution confers on crime victims the rights "to justice and due process" and entitles them to, among other "basic rights," "confer with the prosecution." Tenn. Const. art. I, § 35. The State argues that because Code section 8-7-401 places "at the discretion of the district attorney general" the decision on the "extent of participation" of private counsel employed by "[a] victim of crime or the family members of a victim of crime," *see* T.C.A. § 8-7-401(a), prosecutors are "the de facto advocates for victim rights and interests in criminal proceedings."

In our view, the State's argument misapprehends the role of the district attorney general in a criminal prosecution. The prosecutor is not an advocate for the victim of a crime or the witnesses for the State but is instead the representative of the sovereign state of Tennessee charged with "safeguarding and advocating the rights of the people." *Quillen v. Crockett*, 928 S.W.2d 47, 51 (Tenn. Crim. App. 1995). "District attorneys general are officers of the executive branch, who are entrusted by the citizens of this state with the duty to seek justice." *State v. Head*, 971 S.W.2d 49, 51 (Tenn. Crim.

App. 1997) (citing *State v. Gilliam*, 901 S.W.2d 385, 389 (Tenn. Crim. App. 1995); *State v. Mario Pendergrass*, No. 01C01-9504-CR-00121, 1997 WL 83777 (Tenn. Crim. App., Nashville, Feb. 28, 1997)); *see also State v. Griffis*, 964 S.W.2d 577, 598 (Tenn. Crim. App. 1997) ("The district attorney general is a 'quasi-judicial officer,' who represents the state in criminal prosecutions. However, it is as much the district attorney general's responsibility to enforce the laws as it is to see the accused receives a fair and impartial trial."). Thus, the prosecutor "is in a peculiar and very definite sense the servant of the law, the twofold aim of which is that guilt shall not escape or innocence suffer." *Berger*, 295 U.S. at 88.

Neither the codification of the duties of the district attorney general nor the statutory and constitutional provisions conferring certain rights upon the victims of crime alters the prosecutor's role as the representative of the people of Tennessee. Nor do they endow the State with the power to represent the victim or the witnesses proffered by the State. The State "cannot undertake to act as counsel to its witnesses," even the victim, because the State's "interests and that of its witnesses are not identical." *Nachamie*, 91 F. Supp. 2d at 560–61. The prosecutor's highest interest "in a criminal prosecution is not that it shall win a case, but that justice shall be done." *Berger*, 295 U.S. at 88.

Additionally, the State lacked a sufficient legal relationship with any of the witnesses in this case to allow the State to assert the witnesses' own interests in the subpoenaed material. It is well-established that "a victim in a criminal case does not meet the definition of a 'party'" in a criminal trial. State v. Flood, 219 S.W.3d 307, 314 (Tenn. 2007) (citing City of Chattanooga v. Swift, 442 S.W.2d 257, 258 (Tenn. 1969)); see also State v. Brown, 29 S.W.3d 427, 442 (Tenn. 2000) ("A victim in a sexual assault case is not a party for purposes of a party opponent admission."). Even though the four women have been identified as State's witnesses, "[i]t is hornbook law that generally no party 'owns' a witness." State v. Womack, 591 S.W.2d 437, 444 (Tenn. Ct. App. 1979). We also note that the *Harrison* court did not factor Harrison's psychologist's potential as a witness for either party into its analysis of Harrison's standing to challenge the subpoena issued to his psychologist. Harrison, 270 S.W.3d at 26. In fact, the court found that Harrison had standing to challenge the subpoena despite the fact that he "did not intend to call Dr. Wilson as a witness at trial or to rely on Dr. Wilson's records as evidence in his case-in-chief at trial," id., because he had "a legitimate personal interest in the report and records of the clinical psychologist he retained to ascertain whether he is competent to stand trial and whether he could viably assert an insanity defense," id. at 29.

Finally, we disagree with the State that it has standing to challenge the subpoenas because it is in "the best position to assist the trial court" in determining whether the subpoenas amount to an impermissible "fishing expedition." The record establishes that the information that is the subject of the subpoenas is and always has

been in the exclusive control of the witnesses and the providers. Indeed, the record suggests that the State has gone to great lengths to *avoid* collecting the requested information. Under these circumstances, we cannot see how the State is in a unique position to comment on the content of the information requested. Indeed, the State appears to have engaged in a "hide the ball" strategy which is inimical to the constitutional rights laboriously described above.

Because the State has failed to establish that it has a legitimate interest in the subpoenas at issue, we conclude that the State lacks standing to challenge the subpoenas. In consequence, we reverse the trial court's ruling that the State had standing to challenge the subpoenas issued to the witnesses in this case and affirm the trial court's ruling that the State did not have standing to challenge the subpoenas issued to the service providers.

Although our conclusion that the State lacks standing to challenge the subpoenas renders the remaining issues nonjusticiable, in the interests of judicial economy and potential further appellate review, we address the merits of each party's claim regarding the subpoenas.

### II. Remaining Issues

At this point we provide a brief reminder of the events that led to this The defendants moved the trial court in August 2015 for a court order to accompany subpoenas duces tecum issued to AT&T, Facebook, Twitter, Instagram, Snapchat, and Yik Yak to obtain the electronic communications of four State's witnesses. The defendants argued that the information was relevant, material, necessary to prepare for trial, and not obtainable from any other source. At the hearing, the defendants did not suggest the time period to be covered by the subpoenas or the precise scope of the information requested, asking generally for "social media information and communications material and relevant to the events at issue." Following the hearing, the trial court granted the defendants' request, finding "that specific and articulable facts establish[ed] reasonable grounds to believe that records and information pertaining to designated cellular telephone and social media communications are relevant and material to a pending criminal matter." The subpoenas issued to AT&T demanded essentially every piece of data associated with the cellular telephone accounts of C.C. and Ms. Lawn, including "account records, . . . call detail records . . . , audio recordings, saved contacts, geolocation data, text messages or iMessages sent or received, photographs, video recordings, and voicemail messages" for the period beginning on November 1, 2014, and ending with the date of subpoena compliance. The subpoenas issued to the social media providers similarly asked for every piece of data associated with the accounts of all four witnesses, both the basic non-content information related to the account and the entirety

of the contents of the electronic communications, for the period beginning January 1, 2014, and ending with the date of subpoena compliance.

After the defendants received pushback from four of the social media providers and after learning that AT&T did not possess the content information the defendants desired, the defendants notified the trial court of their intention to issue subpoenas directly to the four witnesses asking for identical information. Those subpoenas issued in September 2015. Only C.C. attempted to comply with the subpoenas, sending printouts from some social media sites accompanied by a letter to the trial court explaining why she was unable to provide more information.

The defendants asked that the witnesses be held in contempt for their failure to fully comply with the subpoenas, and the State moved to quash the subpoenas. The trial court granted the State's motion to quash the subpoenas issued to the four witnesses on grounds that the materials covered by the subpoenas qualified as "statements of witnesses," which cannot be obtained by a Rule 17 subpoena. The court also concluded that the subpoenas were unreasonable and oppressive because the witnesses had been unable to comply despite their best efforts to do so.

In this appeal, the State maintains that the trial court correctly concluded that the requested information qualified as witness statements, rendering them undiscoverable by subpoena, and that the subpoenas were unreasonable and oppressive. The State also contends that the trial court's decision to quash the subpoenas to the witnesses did not violate the defendants' constitutional rights to compulsory process and to present a defense. The defendants assert that the trial court erred on all points.

### A. What Can the Defendants Obtain?

Both the state and federal constitutions guarantee a criminal accused the right to compulsory process for obtaining evidence in his favor. *See* U.S. Const. Amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence."); Tenn. Const. art. I, § 9.

Because [Sixth Amendment] rights are basic to our adversary system of criminal justice, they are part of the 'due process of law' that is guaranteed by the Fourteenth Amendment to defendants in the criminal courts of the States. The rights to notice, confrontation, and compulsory process, when taken together, guarantee that a criminal charge may be answered in a manner now considered fundamental to the fair

administration of American justice—through the calling and interrogation of favorable witnesses, the cross-examination of adverse witnesses, and the orderly introduction of evidence. In short, the Amendment constitutionalizes the right in an adversary criminal trial to make a defense as we know it.

Faretta v. California, 422 U.S. 806, 818 (1975); see also Washington v. Texas, 388 U.S. 14, 18 (1967) ("The right of an accused to have compulsory process for obtaining witnesses in his favor stands on no lesser footing than the other Sixth Amendment rights that we have previously held applicable to the States.").

In constitutional law, as in all things in life, however, there are limits. "The accused does not have an unfettered right to offer [evidence] that is incompetent, privileged, or otherwise inadmissible under standard rules of evidence. The Compulsory Process Clause provides him with an effective weapon, but it is a weapon that cannot be used irresponsibly." *Taylor*, 484 U.S. at 410; *Chambers v. Mississippi*, 410 U.S. 284, 295 (1973) (observing that the criminal defendant's right to present evidence "is not absolute and may, in appropriate cases, bow to accommodate other legitimate interests in the criminal trial process"). Indeed, "[t]he adversary process could not function effectively without adherence to rules of procedure that govern the orderly presentation of facts and arguments to provide each party with a fair opportunity to assemble and submit evidence to contradict or explain the opponent's case." *Taylor*, 484 U.S. at 410-11. "Rules that provide for pretrial discovery . . . . minimize[] the risk that a judgment will be predicated on incomplete, misleading, or even deliberately fabricated" evidence. *Id.* at 411-12.

In addition to the constitutional right to compulsory process, our Code contains a statutory right to compulsory process, *see* T.C.A. § 40-17-105 ("As provided by the Constitution of Tennessee, the accused, in all criminal prosecutions, has a right to meet the witnesses face to face, and to have compulsory process for obtaining witnesses in the accused's favor."), and provides that Rule 17 of the Tennessee Rules of Criminal Procedure "shall govern when a clerk or other authorized officer of the court is required to issue a subpoena in a criminal case in criminal court and the consequences of a person's refusal to appear, testify or produce evidence when subpoenaed," *see id.* § 40-17-122.

Tennessee Rule of Criminal Procedure 17 provides, in pertinent part, as follows:

- (d) Documents and Objects. A subpoena may order a person to produce the books, papers, documents, or other objects the subpoena designates.
- (1) Production to Permit Inspection. The court may direct that the designated items be produced in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.
- (2) Compliance Unreasonable. On motion made promptly and in any event by the time specified in the subpoena for compliance therewith, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive. The court may condition denial of the motion on the advancement by the party in whose behalf the subpoena is issued of the reasonable cost of producing the books, papers, documents, or other objects.

. . . .

- (g) Contempt. When a subpoena is served on a person, the court issuing the subpoena may deem the person's refusal to obey the subpoena to be contempt of court unless the person has an adequate excuse.
- (h) Information not Subject to Subpoena. Statements by witnesses or prospective witnesses may not be subpoenaed from the state or the defendant under this rule, but are subject to production only in accordance with the provisions of Rule 26.2.

## Tenn. R. Crim. P. 17(d), (g)-(h).

Against this backdrop, we begin our analysis with the claim we believe to be the easiest to dispose of: that the subpoenaed materials were "statements by witnesses" and were thus undiscoverable pursuant to the rules of criminal procedure. Rule 17 is "similar to its federal counterpart" in that it "makes it clear that the proper method to secure witness statements *from the opposing side*—either at trial or at a pretrial hearing under Rule 12(b)—is as set forth in Rule 26.2." Tenn. R. Crim. P. 17, Advisory Comm'n Comments (emphasis added). Rule 26.2 provides that

[a]fter a witness other than the defendant has testified on direct examination, the court, on motion of a party who did not call the witness, shall order the attorney for the state or the defendant and the defendant's attorney to produce, for the examination and use of the moving party, any statement of the witness that is in their possession and that relates to the subject matter of the witness's testimony.

Tenn. R. Crim. P. 26.2(a). As used in Rule 26.2, and by extension, Rule 17, the term "witness's statement" means: "(1) A written statement that the witness makes and signs, or otherwise adopts or approves; or (2) A substantially verbatim, contemporaneously recorded recital of the witness's oral statement that is contained in a stenographic, mechanical, electrical, or other recording or a transcription of such a statement." Tenn. R. Crim. P. 26.2(f).

Based upon the plain language of the two rules, neither operates to bar the subpoenas for the electronic communications in this case. First, the defendants did not attempt to subpoena any of the electronic communications "from the [S]tate" as prohibited by Rule 17 because, as the State has made clear, none of the desired communications has ever been in the possession of the State. See Tenn. R. Crim. P. 17(h). Additionally, because the communications have never been in the possession of the State, they do not fall within the purview of Rule 26.2, which only governs the production of "any statement of the witness that is in the [] possession [of the non-moving party] and that relates to the subject matter of the witness's testimony." Tenn. R. Crim. P. 26.2(a). As indicated earlier, the record suggests that the State has gone to great lengths to avoid collecting any of the communications sought by the defendants. Second, the communications do not fall within the definition of "witness's statement[s]" provided in Rule 26.2. Nothing in the record suggests that any of the electronic communications consists of either "[a] written statement that the witness makes and signs, or otherwise adopts or approves" or "[a] substantially verbatim, contemporaneously recorded recital of the witness's oral statement that is contained in a stenographic, mechanical, electrical, or other recording or a transcription of such a statement." See Tenn. R. Crim. P. 26.2(f).

Our conclusion that the rules of criminal procedure do not expressly prohibit the defendants from seeking the electronic communications via Rule 17 subpoena does not end our inquiry.

The Supreme Court has "recognized" that "the subpoena duces tecum" provided for in the federal counterpart to Rule 17 "was not intended to provide a means of discovery for criminal cases" and that "its chief innovation was to expedite the trial by

providing a time and place before trial for the inspection of subpoenaed materials."<sup>13</sup> *Nixon*, 418 U.S. at 698-99 (citing *Bowman Dairy Co.*, 341 U.S. at 220). Importantly, "[a] subpoena for documents may be quashed if their production would be 'unreasonable or oppressive,' but not otherwise." *Id.* at 698. In consequence, the party seeking production of evidence via the federal rule prior to trial must show:

(1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general 'fishing expedition.'

*Nixon*, 418 U.S. at 699-700. To carry this burden, the moving party "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *Id.* at 700. The defendants argue that they have met this burden. The State argues that they have not.

The decision whether to enforce "a pretrial subpoena duces tecum must necessarily be committed to the sound discretion of the trial court since the necessity for the subpoena most often turns upon a determination of factual issues." *Id.*, 418 U.S. at 702.

In *Nixon*, the Special Prosecutor handling the indictment of John N. Mitchell, H. R. Haldeman, John D. Ehrlichman, Charles W. Colson, Robert C. Mardian, Kenneth W. Parkinson, and Gordon Strachan on charges of conspiracy to defraud the United States and obstruction of justice caused to be issued a subpoena directed at President Nixon, who had been named in the indictment as an unindicted co-conspirator, to produce "in advance of the September 9 trial date . . . certain tapes, memoranda, papers, transcripts or other writings relating to certain precisely identified meetings between the President and others." *Nixon*, 418 U.S. at 686, 689. "The Special Prosecutor was able to fix the time, place, and persons present at these discussions because the White House daily logs and appointment records had been delivered to him." *Id.* at 689.

<sup>&</sup>lt;sup>13</sup> Given that Tennessee Rule of Criminal Procedure 17 is adapted from and therefore similar to Federal Rule of Criminal Procedure 17, we see no reason to treat the application of our rule any differently. *See State v. Lori A. Little*, No. M1999-00858-CCA-R3-CD (Tenn. Crim. App., Nashville, Nov. 22, 2000) (stating that Tennessee Rule of Criminal Procedure 17 "is essentially identical to the federal counterpart in the Federal Rules of Criminal Procedure").

The Supreme Court determined that although "the contents of the subpoenaed tapes could not at that stage be described fully by the Special Prosecutor," the evidence offered by the Special prosecutor in the form of "the sworn testimony or statements of one or more of the participants in the conversations as to what was said at the time" as well as "the identity of the participants and the time and place of the conversations," evinced "a sufficient likelihood that each of the tapes contains conversations relevant to the offenses charged in the indictment." *Id.* at 700. The Court also concluded that the Special Prosecutor had made "a sufficient preliminary showing that each of the subpoenaed tapes contains evidence admissible with respect to the offenses charged in the indictment." *Id.* In addition to "valid potential evidentiary uses" for the requested materials, the Supreme Court noted that "the analysis and possible transcription of the tapes may take a significant period of time," which supported their being produced prior to trial. *Id.* at 702.

## With this foundation, we turn to the present case.

With regard to relevancy, the evidence presented by the defendants supports a conclusion that the four witnesses named in the subpoenas communicated electronically, either via text message or social media, about the party where the events transpired and the offenses themselves. Although the defendants cannot describe fully the contents of the electronic communications, the ubiquitous nature of electronic communication and the type of "smart phones" used to send text messages and engage in social media, *see Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (observing that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy"), coupled with the admissions by various witnesses about their electronic communications relevant to the offenses, "permit a rational inference that at least part of the conversations relate to the offenses charged in the indictment," *Nixon*, 418 U.S. at 700.

With regard to admissibility, we observe, as did the Court in *Nixon*, that the requested communications are "a collection of out-of-court statements by declarants who will not be subject to cross-examination." *Id.* That being said, the rules of evidence do not bar the admission of all out-of-court statements so long as they fit within an exception to the hearsay rule. Additionally, as was the case in *Nixon*, the requested materials "may also be admissible for the limited purpose of impeaching the credibility of" any witness who testifies at trial. *Id.* at 701 (observing that "[g]enerally, the need for evidence to impeach witnesses is insufficient to require its production in advance of trial" but pretrial production is justified when "there are other valid potential evidentiary uses for the same material" and the production "may take a significant period of time").

This brings us to the demand included in the subpoenas that C.C. and Ms. Lawn produce their cellular telephones for inspection and examination. Nothing at the hearing on the defendants' motion suggested that the defendants were seeking production of the cellular telephones themselves, and the trial court made no findings in this regard. The defendants presented no evidence of a need for production of the cellular telephones. Indeed, the evidence presented at the hearing and other evidence included in the record indicates that both women had replaced their cellular telephone handsets within days of one another in January 2015 and that C.C. had sold her old handset online, despite expressing to the police that the handset was not in working order, and that Ms. Lawn had disposed of hers as well. Based on these facts, the defendants have failed to establish that pretrial production of the cellular telephone handsets is likely to produce relevant, admissible evidence.<sup>14</sup>

Finally, we observe that although the defendants' arguments, both in their motion and at the hearing, suggested subpoenas for the production of electronic communications about the offenses made during the period of time surrounding the offenses and the ensuing investigation, the subpoenas actually issued in this case lack that same specificity. The subpoenas request from the social media providers and the four witnesses every piece of both content-related and non-content-related electronic communications generated by the four witnesses for the 18-month period prior to the issuance of the subpoenas. This broad, general request spanning a lengthy and openended time frame finds no support in either the case law or the record. As indicated, the defendants have established that some of the witnesses' electronic communications are likely to contain relevant, admissible evidence. The relevant time frame for the

We also question whether the type of inspection of the cellular telephone handsets contemplated by the subpoenas in this case is permissible via a Rule 17 subpoena following the Supreme Court's decision in *Riley*. There, the Court observed that "[t]oday . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate," *Riley*, 134 S. Ct. at 2490 (citing *Ontario v. Quon*, 560 U.S. 746, 760 (2010)), and concluded that the government could not search the contents of a cellular telephone seized incident to an arrest without either obtaining a search warrant or proving that exigent circumstances required the warrantless search of the phone:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

electronic communications of Ms. Lawn, Ms. Boland, and Ms. Tavares, based upon the evidence and argument presented at this stage in the proceedings, would be the period beginning the day of the party and ending when the witnesses were cautioned by the KPD to avoid discussing the offenses on social media. Because of the nature of the relationship alleged between C.C. and Mr. Johnson, the relevant time frame for her electronic communications would be broader, spanning from the beginning of their relationship until she closed her social media accounts.

In summary, the defendants established, under the *Nixon* standard, an entitlement to pretrial production of the electronic communications of each of the witnesses within the above-described relevant time frames. Because the subpoenas actually issued lack specificity as discussed, rendering them overly broad, we would have concluded that the subpoenas should be modified to require the production only of those materials as outlined above had we not previously concluded that the State lacked standing to challenge the subpoenas.

## B. From Whom Can the Defendants Obtain Information?

Having determined what the defendants are entitled to, we now consider from whom they may acquire it.

#### 1. Service Providers

In the trial court, the social media providers responded to the subpoena by letter stating that the terms of the Stored Communications Act ("SCA"), which is part of the Electronic Communications Protection Act ("ECPA"), forbade the disclosure of the contents of the witnesses' electronic communications to the defendants via a Rule 17 subpoena. The record does not contain any objections from either AT&T or YikYak. AT&T did indicate via letter that it did not possess any electronic communications. YikYak indicated that it would comply with the subpoenas. None of the providers joined the State's motion to quash. The trial court concluded that the State lacked standing to challenge the subpoenas to the service providers, and we agree with this ruling, as we held above. Because the trial court found that the State lacked standing to challenge those subpoenas, those subpoenas remain intact, and the court did not consider the application of the SCA at the November 3 hearing that is the subject of this interlocutory appeal. The trial court did, however, conclude following the August 24, 2015 hearing that the defendants could obtain the electronic communications from the service providers under the terms of the SCA. As we indicated before, we are addressing those issues for which the record is adequate for our review both to promote judicial efficiency in this case, which has already been pending for more than two years, and to facilitate potential further appellate review. For those same reasons and to provide guidance to the

trial court upon remand, we will address the application of the SCA to the subpoenas issued to the service providers in this case.

The trial court, the parties, and the providers assumed without analysis that the SCA applied to the social media communications requested by the defendants. As we discuss more fully below, the application of the SCA to these communications is not quite so clear.

"The privacy of stored Internet communications in the United States is governed by" the SCA, which "was enacted in 1986 as part of the Electronic Communications Privacy Act." Orin S. Kerr, A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208 (2004). Because electronic communication development has far outpaced the development of the law in the area of constitutionally-based privacy protections for those communications, Congress passed the SCA to bridge the gap by "creat[ing] a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Id. at 1212. The SCA accomplishes this by limiting "the government's ability to compel providers to disclose information in their possession about their customers and subscribers" and by limiting "the ability of [internet service providers] to voluntarily disclose information about their customers and subscribers to the government." Id. at 1212–13. "The SCA provides privacy protection to communications held" in electronic storage by "providers of electronic communication service . . . and providers of remote computing service." *Id.* at 1213–14.<sup>15</sup>

"The Stored Communications Act is best understood by considering its operation and purpose in light of the technology that existed in 1986" because it "is not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks." William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1204–05 (2010). For this reason, it is necessary to understand how computing operated at that time in order to understand how the SCA might be applied to more recent innovations such as social media networks.

The United States Code defines "electronic communication service" ("ECS") as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Electronic storage is both

 $<sup>^{15}</sup>$  As the author points out, "the distinction that the SCA draws reflects the technology of the 1980s." *Id.* at 1213.

"any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17). Because "Congress explored" the ECS category "primarily through the lens of early electronic mail systems," which "[a]t the time, . . . operated through a fragmented delivery system in which communications were slowly transmitted between the computer servers operated by e-mail providers," the resulting definition of electronic storage is "rather odd" and "much narrower than its name suggests." Robison, *supra*, 1205-06.

The Code defines "remote computing service" ("RCS") as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). "Congress created" this category "to address third-party service providers that offered 'sophisticated and convenient computing services to subscribers and customers from remote facilities." Robison, *supra*, 1206 (quoting S. REP. NO. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555). At the time Congress adopted the SCA, "outsourced computing was a service marketed to 'businesses of all sizes--hospitals, banks and many others,' rather than individual consumers," and, as a result, "[t]he requirements for RCS precisely describe the nature of the commercial relationship that existed at the time of the Act's adoption between the outsourced computing providers and their business clientele." Robison, *supra*, 1207.

A few remaining definitions are in order. Electronic communication is defined as

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title); or
- (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12). "[G]overnmental entity' means a department or agency of the United States or any State or political subdivision thereof." *Id.* § 2711(4). "[C]ontents',

when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

The SCA makes it a crime for anyone to "intentionally access[] without authorization a facility through which an electronic communication service is provided" or "intentionally exceed[] an authorization to access that facility" and use that access to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." *Id.* § 2701(a). This provision is inapplicable "to conduct authorized . . . by the person or entity providing a wire or electronic communications service; . . . by a user of that service with respect to a communication of or intended for that user; or . . . in section 2703, 2704 or 2518 of this title." *Id.* § 2701(c).

Code section 2702, which regulates the voluntary disclosure of information provides, in pertinent part, as follows:

- (a) Prohibitions.--Except as provided in subsection (b) or (c)--
  - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
    - (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
      - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
      - (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
    - (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a

subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

- (b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--
  - (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
  - (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title:
  - (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

. . . .

- (c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--
  - (1) as otherwise authorized in section 2703;
  - (2) with the lawful consent of the customer or subscriber;

. . . .

- *Id.* § 2702(a)-(c). Section 2703, which governs compelled disclosure of electronic communications, provides:
  - (a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of

competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

- (b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--
  - (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
  - (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
    - (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
    - (ii) obtains a court order for such disclosure under subsection (d) of this section;
  - except that delayed notice may be given pursuant to section 2705 of this title.
- (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--
  - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
  - (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of

providing any services other than storage or computer processing.

- (c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
  - (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
  - (B) obtains a court order for such disclosure under subsection (d) of this section;
  - (C) has the consent of the subscriber or customer to such disclosure;
  - (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
  - (E) seeks information under paragraph (2).
- (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the-
  - (A) name;
  - (B) address;
  - (C) local and long distance telephone connection records, or records of session times and durations;
  - (D) length of service (including start date) and types of service utilized;
  - (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
  - (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

- (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.
- (d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

### 18 U.S.C. § 2703(a)-(d).

Importantly, the SCA draws a distinction between content, "the communication that a person wishes to share or communicate with another person," and non-content, "information about the communication that the network uses to deliver and process the content information" such as basic subscriber information. Kerr, *supra*, 1227-28. Kerr explains that "[t]he rules for compelled disclosure operate like an upsidedown pyramid" such that "[t]he higher up the pyramid you go, the more information the government can obtain." *Id.* at 1222.

At the lowest threshold, only a simple subpoena is needed to compel basic subscriber information. Higher up the pyramid, a 2703(d) order compels all noncontent records. A simple subpoena combined with prior notice compels three categories of information: basic subscriber information, plus any opened e-mails or other permanently held files (covered by the RCS rules), plus any contents in temporary "electronic storage" such as unretrieved e-mails in storage for more than

180 days. A 2703(d) order plus prior notice is sufficient to compel all noncontent records, plus any opened e-mails or other permanently held files (covered by the RCS rules), plus any contents in temporary "electronic storage" such as unretrieved e-mails in storage for more than 180 days. Put another way, a 2703(d) order plus prior notice compels everything except contents in temporary "electronic storage" 180 days or less. Finally, a search warrant is needed to compel everything stored in an account.

Id. at 1222-23 (footnotes omitted); see also Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 207-08 (2d Cir. 2016) (hereinafter "Microsoft"). "Data stored by a remote computing service (RCS) . . . receives fewer privacy protections than communications held by an ECS." Robison, supra, 1208.

Because the framework created in the SCA relies entirely on 1986 computing technology, determining the precise scope of its application to the type of social media communications at issue in this case presents difficulties. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (observing that application of the SCA "is a complex, often convoluted, area of the law" and that "the existing statutory framework is ill-suited to address modern forms of communication"). Those

<sup>&</sup>lt;sup>16</sup> The Second Circuit Court of Appeals echoed Kerr's observation that section 2703 "sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government." The court explained,

Basic subscriber and transactional information can be obtained simply with an administrative subpoena. Other non-content records can be obtained by a court order (a "§ 2703(d) order") . . . . The government may also obtain some user content with an administrative subpoena or a § 2703(d) order, but only if notice is provided to the service provider's subscriber or customer. § 2703(b)(1)(B). To obtain "priority stored communications" (our phrase), as described below, the Act generally requires that the government first secure a warrant that has been issued "using the procedures described in the Federal Rules of Criminal Procedure," or using State warrant procedures, both of which require a showing of probable cause. Priority stored communications fall into two categories: For electronic communications stored recently (that is, for less than 180 days) by an ECS, the government must obtain a warrant. § 2703(a). For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer.").

courts faced with the issue have concluded that the SCA is applicable to social media sites and that the SCA prohibits social media sites "from disclosing nonpublic contents without the user's consent." Steven S. Gensler, Special Rules for Social Media Discovery?, 65 Ark. L. Rev. 7, 26–28 (2012); see also Matter of Application of State for Commc'ns Data Warrants To Obtain the Contents of Stored Commc'ns From Twitter, Inc., From Users @ \_ & @ \_, ESS-147-CDW-16 & ESS-148-CDW-16., No. A-3651-15T4, 2017 WL 476218, at \*7 (N.J. Super. Ct. App. Div. Feb. 2, 2017) (observing that "courts have uniformly concluded that communications sent to social media platforms or even private websites are clearly 'electronic communications' under the" SCA). The nuances of that application, however, have varied based upon the facts and circumstances of each individual case. For example, in Crispin v. Christian Audigier, Inc., the court concluded that the SCA applied to Facebook but that Facebook was an ECS as to some electronic communications on Facebook and an RCS as to others. See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980-82 (C.D. Cal. 2010). In Ehling v. Monmouth-Ocean Hosp. Serv. Corp., the court concluded that "Facebook wall posts that are configured to be private meet all four criteria" to qualify as electronic communications held by an ECS. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 667 (D.N.J. 2013). Other courts have concluded without detailed analysis that the SCA applies to social media websites and that those sites may not produce information except as provided by the SCA. See, e.g., People v. Harris, 945 N.Y.S.2d 505, 511 (Crim. Ct. 2012) ("If you look at the purpose and method of Twitter, it is clear to this court that Twitter is a service provider of electronic communication.").

We agree with those courts that have concluded that the SCA is applicable to communications shared on social media websites. Thus, the defendants could only obtain the witnesses' communications from the social media providers if they satisfied the terms of the SCA. Analyzing the defendants' requests using the pyramidal structure outlined above, we easily conclude that the defendants cannot obtain the contents of the witnesses' social media accounts from the social media providers via a Rule 17 subpoena because the SCA requires a warrant to obtain those communications. *Microsoft*, 829 F.3d at 207-08 ("For electronic communications stored *recently* (that is, for less than 180 days) by an ECS, the government *must* obtain a warrant. For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer." (citations omitted)); see also Ryan A. Discovering Facebook: Social Network Subpoenas and the Communications Act, 24 Harv. J.L. & Tech. 563, 568 (2011) ("[T]he government cannot obtain content information from public ECS or RCS providers without a search warrant.").

To obtain any information other than "[b]asic subscriber and transactional information," which "can be obtained simply with an administrative subpoena,"

Microsoft, 829 F.3d at 207, the defendants had to show that (1) a defendant in a criminal case qualifies as a "governmental entity" under the terms of the SCA and (2) that the subpoena and order issued in this case satisfies the requirements of Code section 2703(d). Marc J. Zwillinger, Christian S. Genetski, Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not A Level Playing Field, 97 J. Crim. L. & Criminology 569, 587–88 (2007) (stating that "the court order exception contained in 18 U.S.C. § 2703(d) pertains only to the government and comes into play only when a governmental entity 'offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.' By definition, no criminal defendant or party to civil litigation could make this showing."). At least one court has concluded that "[t]he SCA provides no direct mechanism for access by a criminal defendant to private communication content." Facebook, Inc. v. Superior Court, 192 Cal. Rptr. 3d 443, 450, review granted and opinion superseded sub nom. Facebook v. S.C., 362 P.3d 430 (Cal. 2015). Another court has concluded that "the Office of the Federal Public Defender is not a 'government entity' within the meaning of § 2703." United States v. Amawi, 552 F. Supp. 2d 679, 680 (N.D. Ohio 2008). Observing that the SCA defines that term "as 'a department or agency of the United States or any State or political subdivision thereof," the Amawi court concluded that "[t]he judiciary is not a department or agency of the United States; thus, the judiciary and its components, including the Federal Public Defender, cannot obtain a court order under § 2703(d)." Id.; see also Zwillinger, supra, 594 ("The purpose and plain text of the SCA make clear that the exceptions for governmental entities apply only to Fourth Amendment government actors--investigative agencies and prosecuting attorneys-- and not to criminal defendants, irrespective of whether they happen to be represented by a publicly funded criminal defender's office."). The Amawi court also observed that the SCA "distinguishes between courts, which issue orders, and government entities, which can apply for orders." Id. We find this reasoning sound. Consequently, we would have held, had the issue been justiciable, that the defendants could not obtain any information directly from the social media providers under the terms of the SCA because they do not meet the definition of "governmental entity." See 18 U.S.C. § 2711(4) ("[G]overnmental entity means a department or agency of the United States or any State or political subdivision thereof."); id. at § 2703(d) (stating that a court of competent jurisdiction may issue an order upon an application by a governmental entity); see also Zwillinger, supra, at 584 ("None of the[] exceptions [in the SCA] provide a basis for a disclosure in response to a subpoena served by a criminal defendant, nor a court order secured at the defendant's request."). 17

#### 2. Witnesses

 $<sup>^{17}</sup>$  We caution that our review of the SCA in this part is limited to the issue that has thus far arisen in the present case. We do not mean to suggest that the SCA passes constitutional scrutiny in all respects.

Although the defendants cannot obtain the witnesses' electronic communications directly from the social media providers, nothing prevents them from obtaining the information as outlined above directly from the witnesses themselves. *See* John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU Sci. & Tech. L. Rev. 465, 473 (2011) ("The most effective methods of obtaining discovery of the contents of a party's social networking profile are propounding specific, well-tailored discovery requests to the party himself . . . ."). By its terms, the SCA places limitations only on the service providers and not on the users of social media websites. *See* 18 U.S.C. § 2702(a); § 2703(a). The vast majority of cases make it clear that the type of electronic communications sought in this case fall clearly within the ambit of civil discovery when obtained from the account holder or user, and we see no reason that the same information should not also be available to criminal defendants via a Rule 17 subpoena, provided that they are able to make the showing required by *Nixon*.

Although courts have indicated that privacy considerations may be implicated when dealing with electronic communications, *see*, *e.g.*, *United States v. Warshak*, 631 F.3d 266, 283-88 (6th Circ. 2010), a privacy claim cannot place those communications totally beyond the reach of a criminal defendant who has shown that the communications are likely to contain relevant, material evidence. To hold otherwise would be to apply a sort of privilege to electronic communications that does not exist for other forms of communication, a privilege that would serve only "to withhold evidence that is demonstrably relevant in a criminal trial" and "cut deeply into the guarantee of due process of law and gravely impair the basic function of the courts." *Nixon*, 418 U.S. at 712. "Certain exemptions from" providing evidence "are recognized by all courts," "[b]ut every such exemption is grounded in a substantial individual interest which has been found, through centuries of experience, to outweigh the public interest in the search for truth." *Bryan*, 339 U.S. at 332. As the Supreme Court observed,

We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the

production of evidence needed either by the prosecution or by the defense.

*Nixon*, 418 U.S. at 709. Privileges erected by the Court to place evidence beyond the reach of compulsory process "are designed to protect weighty and legitimate competing interests. . . . Whatever their origins, these exceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth." *Id.* at 709-10. Even where a privilege exists, such as in the case of the presidential communications at issue in *Nixon*, "[t]he generalized assertion of privilege must yield to the demonstrated, specific need for evidence in a pending criminal trial." *Id.* at 713.

The defendants have satisfied the *Nixon* requirements with regard to those electronic communications falling within the relevant time frames outlined above. No evidence suggests that the witnesses enjoy a blanket privilege with regard to their electronic communications.<sup>18</sup>

Moreover, we disagree with the trial court's finding that the subpoenas issued to the witnesses were oppressive. First, the evidence relied on by the court to support this finding, the letter from Ms. Boland's mother, does not indicate anything more than a minor difficulty in obtaining the requested information experienced by one of the witnesses. Ms. Boland's mother complained to the assistant district attorney via email that Ms. Boland and her parents had had to spend several hours during a weekend visit attempting to comply with the subpoena. We hardly think this too onerous a burden when juxtaposed with the defendants' constitutional trial rights. When put in perspective, the expense of a few hours' time and a few dollars are less than "oppressive." Courts have recognized that complying with that "fundamental maxim that the public . . . has a right to every man's evidence," *Bryan*, 339 U.S. at 332, will necessarily involve "personal sacrifice" but that the sacrifice "is a part of the necessary contribution of the individual to the welfare of the public," even when "onerous," *Blair*, 250 U.S. at 281.

#### Conclusion

We hold that the State lacks standing to challenge the subpoenas issued to C.C., Ms. Lawn, Ms. Boland, and Ms. Tavares. The State also lacks standing to challenge the subpoenas issued to any of the service providers in this case. Accordingly, we affirm in part and reverse in part the trial court's November 3 order.

<sup>&</sup>lt;sup>18</sup> We note that although Federal Rule of Criminal Procedure 17 places additional requirements on requests for "the production of personal or confidential information about a victim," *see generally* Fed. R. Crim. P. 17(c), Tennessee Rule of Criminal Procedure 17 does not contain similar requirements.

JAMES CURWOOD WITT, JR., JUDGE