STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS

PROVIDENCE, SC. **SUPERIOR COURT**

(FILED: May 30, 2017)

STATE OF RHODE ISLAND	**:**	
	:	
v.	**:**	**No. P2-2014-3011A**
	:	
ENRIQUE RODRIGUEZ	**:**	

DECISION

K. RODGERS, J. The State of Rhode Island (State) has charged Enrique Rodriguez (Defendant) with one count of possession of child pornography in violation of G.L. 1956 § 11-9-1.3(a)(4) and one count of transfer of child pornography in violation of § 11-9-1.3(a)(2). The issues before this Court center on the issuance of and compliance with an administrative subpoena directed to Verizon Internet Services (Verizon), an internet service provider (ISP), seeking the name and address of the subscriber assigned a particular internet protocol (IP) address which had been involved in the transfer of child pornography. Armed with that subscriber information, law enforcement personnel requested a search warrant for the computer hardware and software maintained at the home that Defendant shared with his wife and children. Defendant now moves this Court to suppress all statements and evidence obtained pursuant to the execution of that search warrant.

Jurisdiction is pursuant to G.L. 1956 § 8-2-15. For the reasons that follow, Defendant's motion to suppress is denied.

I

Facts and Travel

A

The Investigation

In February 2014, Detective Kevin Harris (Det. Harris), a detective with the Coventry Police Department and a member of the Rhode Island Internet Crimes Against Children (ICAC) Task Force,[1] was undercover monitoring a peer-to-peer file-sharing network.[2] On February 28, 2014, Det. Harris identified and observed an IP address[3]—100.40.45.192—sharing numerous files of suspected child pornography. Det. Harris made a direct connection to the IP address and downloaded several child pornography files. Subsequently, Det. Harris used the American

[1] Formed in 2003, Rhode Island's ICAC "is a multi-agency group comprised of sworn federal, state and local law enforcement officials, local prosecution officials, local educators, private information technologists and mental health professionals throughout the State of Rhode Island," and its primary responsibility is to conduct investigations into "Internet-driven crimes against children[.]" *Internet Crimes Against Children Task Force*, State of R.I. State Police Dep't of Public Safety, http://risp.ri.gov/ccu/icac.php (last visited May 12, 2017).

[2] File-sharing software connects users within the peer-to-peer network directly and allows users to download and view files stored on other users' computers in their shared folders. See U.S. v. Abbring, 788 F.3d 565, 566 (6th Cir. 2015). In order to download a file, a user enters a search term which generates a list of files on other computers in the network that match the search term and are available for download. See U.S. v. Conner, 521 F. App'x 493, 494 (6th Cir. 2013). "[U]sers can also view the internet protocol . . . address of the computer from which they are downloading files." Id. at 495.

[3] An IP address is a unique number assigned to a subscriber by an ISP that allows for access to the Internet. See U.S. v. Featherly, 846 F.3d 237, 238 (7th Cir. 2017). "Any computer from which a person accesses the internet is assigned an IP address, which may be either 'static' (remain constant) or 'dynamic' (change periodically)." Kilmas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 273 (6th Cir. 2006). When a person types a website name into an Internet browser, their IP address connects with the website's IP address and allows for the transmission of information between the two sources. Id.

Registry of Internet Numbers to determine that Verizon[4] was the owner of that specific IP address.

B

The Administrative Subpoena

At Det. Harris' request, Colonel Steven G. O'Donnell (Col. O'Donnell), Superintendent of the Rhode Island State Police, issued an administrative subpoena to Verizon Legal Compliance, dated March 3, 2014, requesting basic information associated with that IP address. Ex. 2 to Def.'s Mem., Admin. Subpoena. Specifically, the administrative subpoena requested "non-content subscriber information" including the "name, address, IP address log, and telephone number" associated with the IP address. Id. The administrative subpoena directed Verizon to provide subscriber information that was linked to IP address 100.40.45.192 between 12:00 AM and 11:59 PM on March 1, 2014. Id. The administrative subpoena informed Verizon that the Rhode Island State Police were "conducting an investigation in our state with reference to possible illegal activity[.]" Id. It was issued by Col. O'Donnell to Verizon pursuant to G.L. 1956 § 39-2-20.1[5] and requested that Verizon forward the information to Det. Harris. The

[4] In order to access the Internet, an individual must contract with an ISP, such as Verizon. See State v. Reid, 194 N.J. 386, 390, 945 A.2d 26, 28 (2008). To set up an account with an ISP, an individual must disclose personal information—subscriber information—to the ISP, such as his or her name, payment information, address, and phone number. Id. The ISP then assigns an IP address to the subscriber allowing for his or her interaction over the Internet with other computers. Id. Most subscribers "lease" an IP address from an ISP as part of their service package. Id. at 391, 945 A.2d at 28. An IP address can be changed by the ISP at any time. Id. In the case of Verizon, subscriber information is stored by Verizon as business records "to establish, monitor and maintain [a subscriber's] account and billing records; measure credit and payment risk; provide account-related services; [and] deliver and maintain . . . products and services[.]" Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at (unnumbered) page 2.

[5] Section 39-2-20.1(b)(1) provides, in pertinent part,

> "[a]n internet service provider . . . shall disclose subscriber account information consisting of the name, address, IP address, and telephone numbers associated with the account to the attorney

administrative subpoena also directed Verizon to refrain from notifying the subscriber about the subpoena "since it would interfere with an ongoing criminal investigation." Id.

While Det. Harris awaited a response from Verizon, Detective Lieutenant Chris Brooks (Det. Lt. Brooks), a member of the Woonsocket Police Department and the ICAC Task Force, viewed the files that Det. Harris downloaded and determined that the images shared by the IP address constitute child pornography.

On March 13, 2014, Verizon responded to the administrative subpoena and provided the requested information, including the subscriber's name and address: Yudis Rodriguez, 282 Asylum Street, Woonsocket, Rhode Island 02895. Det. Lt. Brooks and another member of the ICAC Task Force, Detective Damien Longo (Det. Longo) of the Rhode Island State Police, confirmed that Yudis Rodriguez was the owner of 282 Asylum Street, a single-family home.

C

The Search Warrant

On March 31, 2014, Det. Lt. Brooks applied for and obtained a search warrant. The search warrant permitted the search and seizure of Yudis Rodriguez, her residence, any and all computer hardware, computer software, computer-related documentation, records, documents, and material related to child pornography, as well as passwords or other data security devices. The search warrant allowed for an on-site forensic preview and off-site forensic analysis of the seized evidence.

> general or to the superintendent of the Rhode Island state police upon proper service, and with certification under oath by the attorney general or by the superintendent of the Rhode Island state police, that the information is necessary for an officially documented criminal investigation or prosecution of criminal complaint based on probable cause relating to" any one of over a dozen criminal offenses, including child pornography. Sec. 39-2-20.1(b)(1).

On April 1, 2014, Det. Lt. Brooks and Det. Longo executed the search warrant along with several other members of the ICAC Task Force and two uniformed State Troopers. Upon entering the residence at 282 Asylum Street, Det. Longo informed Yudis Rodriguez that they had a search warrant for child pornography in the home. Yudis Rodriguez's husband, Enrique Rodriguez (Defendant), her son David Rodriguez, and her two daughters, ages fourteen and nine, were also in the home at the time.

Det. Longo first spoke to David Rodriguez individually, who denied any use of file-sharing software. Next, Det. Longo spoke with Defendant individually about any use of the file-sharing software called Ares.[6] Defendant responded that he was familiar with Ares and had used the software to download music. At that point, Det. Longo read Defendant his Miranda warnings and advised him that he was a suspect in a child pornography investigation. See Miranda v. Arizona, 384 U.S. 436, 456, 467, (1966). In response, Defendant stated that he understood his rights and acknowledged the same by signing the rights form.

After signing the rights form, Defendant again told Det. Longo that he installed the Ares software to download music on the Gateway computer located in the kitchen. Defendant later stated to Det. Longo that he accidentally downloaded and viewed child pornography. Defendant added that he told his wife he accidentally downloaded child pornography when he was trying to download music. Separately, Yudis Rodriguez informed Det. Longo that she found child pornography on the computer and confronted Defendant.

While Det. Longo spoke with Defendant, his wife, and son, other members of law enforcement searched the house. Special Agent Fred Mitchell, a forensic analyst with the United

[6] "Ares is a free open source file-sharing bittorrent p2p client with a powerful search [that] works behind firewalls." *Ares Galaxy: Filesharing-Bittorrent p2p client for Windows*, https://aresgalaxy.io (last visited May 12, 2017).

States Secret Service, uncovered numerous videos of child pornography saved to a folder on the Gateway desktop computer. After this discovery, Det. Longo again spoke with Defendant about the ongoing investigation, and Defendant admitted to intentionally downloading and viewing child pornography. Defendant was placed under arrest and transported to State Police Headquarters. Officers seized several pieces of digital media from the home, including a cell phone, Gateway desktop computer, and two thumb drives.

On July 16, 2014, a forensic examination of the seized evidence uncovered fourteen videos and over 6000 images considered by law enforcement to be child pornography. In addition, the examination confirmed that the Ares peer-to-peer file-sharing software was used to download those images and videos.

D

Subscription and Verizon's Privacy Policy

In an affidavit dated March 8, 2017 and signed and sworn under penalties of perjury, Yudis Rodriguez stated that Defendant is her husband. Y. Rodriguez Aff., ¶ 1. She also stated that while the Verizon subscriber information was in her name alone, Defendant "assisted in all payments and enjoyed mutual access to the internet on our household computer."[7] Id. at ¶ 5.

The contractual relationship between a subscriber of Internet services and Verizon is governed in part by Verizon's privacy policy. Verizon's privacy policy informs subscribers about the information Verizon collects and stores, how they use it, and options regarding its uses of that collected information. See Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at

[7] This Court assumes, without expressly deciding, that Defendant's interest in the IP address assigned to his wife is the same as his wife's interest.

(unnumbered) page 2[8]. Specifically, Verizon collects from its subscribers the subscriber's name, contact information, driver's license number, Social Security Number, and payment information. Id. The policy also states that Verizon collects:

> "[s]ervice usage information [such as] call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information and identifiers, service options [chosen by a subscriber], mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, TV and other video viewership . . ." Id.

Verizon uses this information "to establish, monitor and maintain [a subscriber's] account and billing records; measure credit and payment risk; provide account-related services; deliver and maintain [a subscriber's] products and services; help . . . with service-related issues or questions; manage and protect [Verizon's] networks, services and users from fraudulent, abusive, or unlawful uses[.]" Id.

The policy also includes a section dedicated to "Working together to keep children safe." Id. at (unnumbered) page 13. Verizon explains that it "must be vigilant in protecting the safety and privacy of children online." Id. Within this section, Verizon further states:

> "[r]egrettably, there are those who use the Internet to view, store and distribute child pornography (or who engage in other types of illegal activity involving children). Child pornography is subject

[8] In support of his Motion to Suppress, Defendant attached a full Verizon privacy policy which indicates 2017 as the policy's copyright year. The privacy policy that is currently online notes that it was updated in February 2017. See *Privacy Policy*, Verizon, http://www.verizon.com/about/privacy/full-privacy-policy (last visited May 17, 2017) ("Protecting our customers' privacy is an important priority at Verizon and we are committed to maintaining strong and meaningful privacy protections. The privacy of your information is a significant responsibility and we value the trust you place in us."). A "Recent changes" section of the online version of the privacy policy includes a summary of changes dating back to November 2016, none of which appear to be pertinent to the matter before this Court. Id. at § Recent changes. For purposes of deciding the Motion to Suppress, this Court will refer to Verizon's privacy policy provided by Defendant. See generally Ex. 1 to Def.'s Mem., Verizon Privacy Policy.

> to severe criminal penalties and using the Verizon network to view, store or distribute it violates our service contracts. The Verizon network may not be used by customers in any manner for the storage, transmission or dissemination of images containing child pornography and we will report any instances of such activity of which we become aware to the appropriate . . . authorities." Id. (emphasis added).

The Verizon privacy policy further notes that Verizon "may be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas[.]" Id. at (unnumbered) page 5. The policy explains that this disclosure is "to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of [the] subscription to [Verizon's] products and services and to protect [Verizon's] network, services, devices and users from such use[.]" Id. at (unnumbered) page 9.

II

Standard of Review

The Fourth Amendment to the United States Constitution provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[9] It is well settled that in order to successfully invoke the protections of the Fourth Amendment against unreasonable searches and seizures, a defendant bears the burden of establishing the requisite standing to challenge the legality of the search. State v. Patino, 93 A.3d 40, 51 (R.I. 2014) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)). Whether a defendant has standing is a two-tiered analysis: "(1) [he or she] has a reasonable expectation of privacy in the areas searched or the items seized, and (2) society is prepared to accept the expectation of privacy as objectively reasonable." U.S. v. Wheelock, 772 F.3d 825, 828 (8th Cir.

[9] Article I, Section 6 of the Rhode Island Constitution, protecting against illegal searches and seizures, is virtually identical and provides "[t]he right of the people to be secure in their persons, papers and possessions, against unreasonable searches and seizures, shall not be violated . . . ." R.I. Const. art. 1, § 6; see State v. Patino, 93 A.3d 40, 51 n.19 (R.I. 2014).

2014) (internal quotations omitted); Patino, 93 A.3d at 53. The Rhode Island Supreme Court has gone on to identify a number of additional factors to consider when evaluating the objectively reasonable prong of the standing analysis, including '"whether [defendant] possessed or owned the area searched or the property seized; his or her prior use of the area searched or the property seized; the person's ability to control or exclude others' use of the property; and the person's legitimate presence in the area searched."' State v. Linde, 876 A.2d 1115, 1127 (R.I. 2005) (quoting State v. Verrecchia, 766 A.2d 377, 382 (R.I. 2001)).

In order to establish standing to challenge the constitutionality of a statute, a defendant must demonstrate "not only that he suffered actual personal injury traceable to the challenged action but that he [was] in the zone of interest the statute is meant to protect." U.S. v. Moffett, 84 F.3d 1291, 1293 (10th Cir. 1996); see also MacDonald v. Moose, 710 F.3d 154, 162 (4th Cir. 2013) (holding that "[a] party has standing to challenge the constitutionality of a statute only insofar as it has an adverse impact on his own rights").

III

Analysis

Defendant now seeks to suppress any statements obtained and evidence seized during the execution of the search warrant. He contends that the statements and evidence should be excluded from trial under the Fourth Amendment because (1) the administrative subpoena issued to Verizon constituted an unreasonable search; (2) the administrative subpoena itself was invalid; and (3) the statutory authority for issuing the administrative subpoena, § 39-2-20.1, is unconstitutional.

Defendant asserts broad privacy and technology arguments in an effort to persuade this Court to increase Fourth Amendment privacy safeguards under the Rhode Island Constitution.

However, this Court's review is narrow and those generalized arguments fail under the facts of this case. The central question is whether Defendant's Fourth Amendment rights were violated when police used an administrative subpoena to obtain subscriber information, provided by Defendant's wife to Verizon to obtain household Internet access, linked to an IP address, which police observed to have publicly shared child pornography on a peer-to-peer network.

A

Standing

1

Subjectively Reasonable Expectation of Privacy

Defendant baldly contends that he has taken no actions to expose the IP address he shared with his wife or their subscriber information to plain view and, therefore, has established his subjective interest in the privacy of that subscriber information. However, the subjective component of the two-prong test of reasonable expectation of privacy fails in this case for two reasons: (1) Verizon's privacy policy; and (2) the manner in which Defendant shared files using the IP address assigned to his family subscription.

Verizon's privacy policy explicitly informs a subscriber that if its services are used for child pornography, the service contract would be broken and Verizon would report the activity to law enforcement.[10] Additionally, if a subpoena is received, Verizon would disclose personally identifiable information to comply. Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at (unnumbered) pages 5, 13. Here, Defendant used the Verizon IP address for illegal purposes that Verizon explicitly forewarned would trigger disclosure to law enforcement. While Defendant's

[10] Federal law enacted in 2008 also requires an ISP to disclose known violations of child pornography to the CyberTipline of the National Center for Missing and Exploited Children. 18 U.S.C. § 2258A(a). An ISP's failure to report such violations triggers fines of up to $150,000 for the first offense and $300,000 for subsequent offenses. Id. at § 2258A(e).

content-based information, such as Internet-search history or email messages, is protected by the Fourth Amendment, his non-content subscriber information is afforded fewer protections.[11] See U.S. v. Hambrick, 225 F.3d 656, at * 4 (4th Cir. 2000) (distinguishing between the content of electronic communications, which is protected, and non-content information, including a subscriber's IP address and corresponding identity, which is not). Thus, in light of Verizon's privacy policy, even if Defendant did have a subjective expectation of privacy in the Verizon subscriber information, his expectation was not reasonable.

Defendant further vitiated any subjective privacy expectation by using peer-to-peer file-sharing software. During the execution of the search warrant, Defendant told police that he used Ares file-sharing software. This type of software is "expressly designed to make files on a computer available for download by the public, including law enforcement." U.S. v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013); see also Mark J. Pesando, 50 Am. Jur. 2d Lewdness, Indecency, Etc. § 33 (law enforcement software that monitors and collects files on peer-to-peer networks does not offend the Fourth Amendment because the files are publicly shared). The Ares software "permits users to download and view files stored on other users' computers in their shared folders." U.S. v. Abbring, 788 F.3d 565, 566 (6th Cir. 2015). Unlike other file-sharing software, Ares does not give users the option to disable the automatic sharing feature,

[11]Courts and the legislature have distinguished between the content of electronic communications, which is protected, and non-content information, including a subscriber's IP address and corresponding identity, which is not. See U.S. v. Hambrick, 225 F.3d 656, at * 4 (4th Cir. 2000); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005); 18 U.S.C. § 2703. The Federal Stored Communications Act (SCA) within the Electronic Communications Privacy Act requires ISPs to disclose subscriber information to the government pursuant to an administrative subpoena authorized by Federal or State statute because such basic information is considered non-content and therefore "less private than other records." 18 U.S.C. § 2703(c)(2); see Sams v. Yahoo! Inc., 713 F.3d 1175, 1179-80 (9th Cir. 2013). This distinction is also reflected in Rhode Island's § 39-2-20.1, which only imposes a duty on ISPs to disclose non-content subscriber information.

thereby providing even less privacy. Id. Users of file-sharing software search each other's computers for files they are looking for and can download those files directly. Id. When a person uses these types of file-sharing services, it is akin to "leaving one's documents in a box marked 'free' on a busy city street." Clifford Fishman & Anne McKenna, Wiretapping and Eavesdropping, § 23:25 (2016). In this case, Defendant's expectation of privacy is not lost merely because he used the Internet, but his privacy expectation is defeated by the manner in which he used the Internet—through peer-to-peer software which opens up his computer files for others to access at will, including law enforcement. See id.

Det. Harris observed the IP address assigned to Defendant's household share child pornography openly over the Ares peer-to-peer network. Because Defendant admitted that he used peer-to-peer software—exposing his computer to unknown others—any reasonable expectation of privacy in his computer and its contents was vitiated. See U.S. v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); Conner, 521 F. App'x at 497 (holding that exposure of information through file-sharing software or a peer-to-peer network "defeats an objectively reasonable expectation of privacy under the Fourth Amendment" and renders any subjective expectation of privacy unreasonable); Wheelock, 772 F.3d at 828. Additionally, by using the Ares network, Defendant "assum[ed] the risk" that law enforcement might observe his illegal activity. Patino, 93 A.3d at 56 (holding that when a person sends a text message "he assumes the risk that his confidant will reveal that information to the authorities" defeating any reasonable expectation of privacy) (internal citation omitted).

For these reasons, this Court finds that any subjective expectation of privacy that Defendant claims to have possessed regarding the Verizon subscriber information is unreasonable and does not trigger Fourth Amendment protections.

2

Objectively Reasonable Expectation of Privacy

i

Federal Precedent

This Court is not persuaded that society is prepared to accept as private, information that Defendant knowingly exposed to the public. See Hambrick, 225 F.3d 656, at *2. Information is not protected under the Fourth Amendment when voluntarily turned over to third parties. Id. at *3.

In Wheelock, the local police department observed through investigative software that child pornography could be downloaded from a particular IP address. 772 F.3d at 827-28. Pursuant to state statute, law enforcement sent an administrative subpoena to Comcast Communications, the ISP for the IP address, requesting subscriber information. Id. Comcast complied with the administrative subpoena, and police obtained a search warrant using the subpoenaed subscriber information. Id. The execution of the search warrant uncovered hard drives, DVDs, and CDs containing child pornography, in addition to a computer actively downloading suspected child pornography with peer-to-peer file-sharing software. Id. In his challenge to the district court's denial of his motion to suppress, Wheelock argued that law enforcement's use of an administrative subpoena to obtain subscriber information violated his Fourth Amendment privacy rights. To support his contention that the Eighth Circuit should abandon the third-party doctrine in its Fourth Amendment analyses, Wheelock cited to Justice Sotomayor's concurring opinion in U.S. v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring), in which she speculated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" because it is "ill suited to the digital age." Wheelock, 772 F.3d at 829. Recognizing that

in the future the United States Supreme Court may review and revise the third party doctrine's limitations on Fourth Amendment protections in light of unfolding digital privacy concerns, the Wheelock Court nonetheless relied on clear federal precedent that no reasonable expectation of privacy exists for subscriber information. Id. (noting that '"[e]very federal court to address this issue has held that subscriber information provided to an internet [service] provider is not protected by the Fourth Amendment's privacy expectation"') (quoting Perrine, 518 F.3d at 1204-05); see also Hambrick, 225 F.3d 656, at *4 (holding that a person has no privacy interest in non-content service account information provided to an ISP to set up an email account); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (concluding that because subscriber information was conveyed to a third party, no privacy interest existed for Fourth Amendment purposes); Conner, 521 F. App'x at 498 (determining that no reasonable expectation of privacy existed in child pornography files that police obtained through defendant's use of peer-to-peer sharing services).

Similar to the defendant's arguments in Wheelock, Defendant here urges this Court to disregard clear federal precedent that subscriber information is not protected under the Fourth Amendment in light of Justice Sotomayor's concurring opinion in Jones. See Wheelock, 772 F.3d at 829; Jones, 565 U.S. at 417. Defendant also cites to Riley v. California, 134 S. Ct. 2473 (2014) to further support his argument that the law is trending toward greater privacy protections when it comes to technology. Defendant contends that the Riley decision demonstrates the United States Supreme Court's readiness to protect citizens' digital property privacy interests. See id. at 2495. In Riley, the Supreme Court held that police officers are required to obtain a warrant prior to accessing the contents of an arrestee's cell phone. Id. The facts of Defendant's case, however, differ greatly from those before the Riley Court. Id. at 2477. For instance, the information accessed instantaneously from a cell phone—which the Riley Court described as a

minicomputer—is infinitely vast. Id. at 2489. Whereas, in this case, the administrative subpoena's request to Verizon for basic subscriber information—name and address—associated with an IP address is markedly more limited in scope. Therefore, like the Wheelock Court, this Court finds that while greater protections for privacy in the technology context may come to be in the future, this Court will not stray from the clear federal precedent that presently holds that there is no reasonable expectation of privacy in subscriber information. 772 F.3d at 829.

ii

The Extension of Rhode Island Privacy Protections

Rhode Island, in its reasonable expectation of privacy analysis, focuses on the element of control over information. Patino, 93 A.3d at 56. In Patino, the Supreme Court held that a person relinquishes control, thereby vitiating any reasonable expectation of privacy, when he or she sends a text message to another person. Id. at 57. The Supreme Court further explained that when a person sends a text message, "he assumes the risk that his confidant will reveal that information to the authorities" and, thus, defeats any reasonable expectation of privacy. Id. at 56 (internal citation omitted). When making a reasonable expectation of privacy determination, our Supreme Court has also considered '"whether the suspect possessed or owned the area searched or the property seized; his or her prior use of the area searched or the property seized; the person's ability to control or exclude others' use of the property; and the person's legitimate presence in the area searched."' Id. at 52 (quoting Verrecchia, 776 A.2d at 382).

In this case, Defendant's subscriber information is under Verizon's complete control for its own internal business processes, such as billing. Id.; see Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at (unnumbered) page 2 (explaining that Verizon uses subscriber information "to establish, monitor and maintain [a subscriber's] account and billing records; measure credit and

payment risk; provide account-related services; deliver and maintain . . . products and services"). While Defendant certainly has control over his own identity, he and his wife leased the IP address from Verizon and voluntarily provided Verizon with the subscriber information in order to obtain Internet services for the household. Additionally, Verizon uses the subscriber information for its own internal business processes. Id. Verizon can change the IP address at will, further demonstrating that Defendant and his wife lack control over their IP address. Therefore, Defendant lacks control over the subscriber information, and no objectively reasonable expectation of privacy exists that society is prepared to accept. See Patino, 93 A.3d at 56.

Notwithstanding the Rhode Island Supreme Court's reliance on the element of control, Defendant urges this Court to anticipate and extend greater privacy protections to Defendant's subscriber information. Defendant cites to a New Jersey Supreme Court decision to further support his argument that Rhode Island should increase protections under its own Constitution. State v. Reid, 194 N.J. 386, 399, 945 A.2d 26, 33-34 (2008). The New Jersey Supreme Court found that a reasonable expectation of privacy existed in subscriber records under New Jersey law. Id. It is well established in New Jersey that disclosure of information to a third party does not defeat one's Fourth Amendment privacy interest. Id. In contrast, the Rhode Island Supreme Court has examined privacy expectations under the Fourth Amendment according to the third-party doctrine, focusing on the element of control over the place searched or item seized. Patino, 93 A.3d at 56. This Court declines to follow New Jersey precedent when Rhode Island precedent utilizes the third-party doctrine, and the subscriber information at issue in this case was readily provided to Verizon by Defendant and his wife to allow Verizon to conduct its

internal business and provide Internet services to Defendant's household. See id. at 49; Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at (unnumbered) page 2.

In Defendant's quest for the extension of greater protections under the Rhode Island Constitution, he also relies upon the Rhode Island Supreme Court's decision in Pimental v. Dep't of Transp., 561 A.2d 1348, 1352 (R.I. 1989). In Pimental, the Court declared that roadblocks or checkpoints aimed at apprehending persons driving while intoxicated violate art. 1, sec. 6 of the Rhode Island Constitution. Id.; cf. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (finding that properly conducted roadblocks are constitutional under the United States Constitution). The Pimental Court held that "[i]t is illogical to permit law enforcement officers to stop fifty or a hundred vehicles on the speculative chance that one or two may be driven by a person who has violated the law in regard to intoxication" and that "less intrusive means exist to address the drunk-driving problem" than sobriety checkpoints. Pimental, 561 A.2d at 1352. The Court reasoned that "[w]e are confident that trained law enforcement officials can spot violators without having to stop all traffic." Id. Without roadblocks, officers would permissibly only stop vehicles based on probable cause or at least individualized articulable suspicion that the driver is intoxicated. Id. Overall, the Pimental Court held that roadblocks "diminish the guarantees against unreasonable searches and seizures contained in the Rhode Island Constitution." Id.

The facts in the instant matter do not warrant an extension of constitutional protections as the Pimental Court found was needed in striking down roadblocks. See id. When police monitor peer-to-peer networks for child pornography, reasonable and individualized suspicion that the person using the IP address is involved in child pornography exists because they observe the illegal activity firsthand. After monitoring the peer-to-peer network and identifying the IP address, the only additional piece of information Det. Harris needed to obtain in order to request

a search warrant was the name and address of the individual assigned the IP address. In the investigation of child pornography crimes, if police are not allowed access to basic subscriber information needed to link an identity with an IP address known to be involved in sharing, transmitting, or downloading child pornography, an investigation "is likely to hit a dead end and a child in danger may not be rescued." Staff of H. Comm. on Energy and Commerce, 109th Cong., Rep. on Sexual Exploitation of Children Over the Internet 3 (Comm. Print 2007). Thus, without the IP address's associated subscriber information, when law enforcement agents observe a particular IP address involved in child pornography activities, the individual using that IP address would remain anonymous, frustrating law enforcement's ability to investigate crimes involving child pornography. Id. Since its emergence in the early 1990's, the Internet has made law enforcement's battle against child pornography increasingly formidable for numerous reasons, including:

> "(1) the Internet provides an anonymous and quick method of transporting images . . .; (2) the Internet provides an anonymous forum for pedophiles to communicate and connect with one another; and (3) digital photographs preclude the need for going to a photography shop to have the photographs developed, hence making the transmission of the images more private." Id. at 7-8.

This Court finds that the investigation of child pornography on the Internet is sufficiently distinct from the prevention of drunk driving through the use of sobriety checkpoints. Accordingly, this Court declines Defendant's invitation to extend greater protections for basic subscriber information under the Rhode Island Constitution.

iii

The Statute Does Not Offer an Objectively Reasonable Expectation of Privacy

Defendant next contends that the Rhode Island General Assembly's mere enactment of § 39-2-20.1 establishes an objectively reasonable expectation of privacy in subscriber information. Notably, § 39-2-20.1 requires that upon receipt of an administrative subpoena, Verizon disclose non-content subscriber information to the Rhode Island State Police Superintendent or Attorney General. The focus of § 39-2-20.1 is not privacy, but an ISP's duty to disclose and its protection from liability when disclosure is made in strict compliance with the statute. Sec. 39-2-20.1(g). The Kelsey Smith Act, also found in Title 39, Chapter 2 entitled "Duties of Utilities and Carriers," is similarly aimed at shielding communications carriers[12] from liability upon disclosure of requested information to law enforcement—including name, address, telephone number, and, in an emergency situation, device location information. Sec. 39-2-20 (providing that "[n]o cause of action shall lie in any court against any communications common carrier . . . for furnishing or disclosing the information in accordance" with the statute). These statutes do not permit or require disclosure of content-based information, nor do they create any expectation of privacy in non-content subscriber information.

By way of comparison, our General Assembly is fully capable of creating a statutory right to privacy that extends beyond a liability-protection or a duty-to-comply statute. In the healthcare context, the statute governing patient privacy is the Rhode Island Confidentiality of

[12] A communications carrier is "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy . . . ." 47 U.S.C. § 153(11); see also G.L. 1956 § 12-5.1-1 (providing that "Communications common carrier" has the same meaning given to the term "common carrier" by 47 U.S.C. § 153(11)). For example, providers of telecommunications services are considered common carriers under Title II of the federal Communications Act, while providers of information services are not. Nat'l Ass'n of Regulatory Util. Comm'rs v. Fed. Commc'ns Comm'n, 851 F.3d 1324, 1325 (2017) (citing 47 U.S.C. § 153(24), (53)).

Health Care Communications and Information Act (CHCCIA). G.L. 1956 §§ 5-37.3-2, et seq. The CHCCIA "represents the General Assembly's attempt to create a physician-patient privilege that had not existed previously in the state of Rhode Island" and "provid[es] a means by which information could be disclosed in a judicial proceeding without obviating a patient's right to contest the disclosure." In re Doe, 717 A.2d 1129, 1132-33 (R.I. 1998). The purpose of the CHCCIA "is to establish safeguards for maintaining the integrity of confidential health care information that relates to an individual." Sec. 5-37.3-2. The CHCCIA "strikes a permissible balance between a party's interest in maintaining the confidentiality of his or her personal health care records and the court's need to access relevant information." In re Doe, 717 A.2d at 1133. The statute confers a presumption in favor of the patient's privacy, but this presumption may be overcome by "demonstrating a particularized need that clearly outweighs the privacy interest of the interest of the individual." Id. at 1133-34 (citing § 5-37.3-6.1). As part of its safeguards, CHCCIA gives patients the opportunity to challenge the validity of a subpoena. Id. at 1135; § 5-37.3-6.1(b) and (d) (providing that within twenty days of the service of a subpoena, a patient may file a motion to quash, which a court shall grant, unless the requesting party can show "that there is reasonable ground to believe the information being sought is relevant to the proceedings, and the need for the information clearly outweighs the privacy interest of the individual"). Yet, the General Assembly has included no such protections for Internet subscribers and their subscriber information in § 39-2-20.1, leading this Court to conclude that the General Assembly intended that no such privacy interest exists.

iv

Verizon's Privacy Policy and File Sharing

For the same reasons that Verizon's privacy policy does not support a subjectively reasonable expectation of privacy in subscriber information, it also fails to establish any objectively reasonable expectation of privacy that society is prepared to accept. Verizon's privacy policy explicitly informs subscribers that it will report any illegal activity to law enforcement, including child pornography, and will disclose personally identifiable information to comply with subpoenas. Ex. 1 to Def.'s Mem., Verizon Privacy Policy, at (unnumbered) pages 5, 13. The policy reflects society's acquiescence that when Internet services are used for illegal purposes, such as child pornography, some privacy expectations should be dispensed with in order to better protect children from sexual exploitation. Additionally, Defendant's use of the Ares file-sharing software made his files, along with those containing child pornography, available for download by the public, including Det. Harris. The manner in which Defendant exposed his IP address to other Ares users to share child pornography defeated any reasonably objective expectation of privacy that society is prepared to accept and protect.

* * *

For all the foregoing reasons, this Court finds that Defendant has not established either a subjectively or objectively reasonable expectation of privacy in the subscriber information held by Verizon. Accordingly, Defendant lacks standing to challenge the search under the Fourth Amendment. See Patino, 93 A.3d at 56.

B

Administrative Subpoena

Defendant next contends that the administrative subpoena issued by the Rhode Island State Police was deficient because it failed to meet all the requirements outlined in § 39-2-20.1(b). Defendant argues that the search warrant containing the subscriber information is also rendered invalid, and that the Fourth Amendment exclusionary rule bars the use of all evidence seized and statements obtained at trial.

Section 39-2-20.1(b) provides that an ISP shall disclose subscriber information to the Superintendent of the Rhode Island State Police "upon proper service, and with certification under oath by the attorney general or by the superintendent of the Rhode Island state police, that the information is necessary for an officially documented criminal investigation or prosecution of criminal complaint based on probable cause" and related to any one of over a dozen criminal offenses, including child pornography. In this case, the administrative subpoena was faxed to Verizon Legal Compliance, thus satisfying the statutory requirements for proper service. Sec. 39-2-20.1(a)(5) (providing that delivery by facsimile constitutes proper service). The administrative subpoena was issued as part of a child pornography investigation, included the criminal investigation case number, and informed Verizon that "[t]he information is necessary for an investigation and prosecution of criminal violations of Rhode Island law." Ex. 2 to Def.'s Mem., Admin. Subpoena. In addition, the administrative subpoena was signed by the head of the state police, Col. O'Donnell. Id. However, it includes no certification under oath that the

information requested was pursuant to a criminal investigation based upon probable cause, nor is there reference to a specific statutory violation that was being investigated. See id.[13]

This Court finds that even if the administrative subpoena was invalid under § 39-2-20.1(b), Defendant lacks standing to challenge the administrative subpoena under the Fourth Amendment because he has no reasonable expectation of privacy in the subscriber information sought by the administrative subpoena. See Rakas v. Illinois, 439 U.S. 128, 134 (1978). "[O]nly defendants whose Fourth Amendment rights have been violated [can] benefit from the [exclusionary] protections." Id. In Hambrick, the Attorney General conceded that the subpoenas used to obtain subscriber information—associated with a screen name police knew to have engaged in child exploitation activities—were invalid. See 225 F.3d 656, at *2. Despite any deficiencies in the subpoena, the Fourth Circuit concluded that "[t]he invalidity of the subpoena . . . does not trigger the application of the Fourth Amendment" because the defendant had no privacy interest in the non-content subscriber information obtained through the subpoena. Id. at *4.

Here, Defendant has no reasonable expectation of privacy in the subscriber information and therefore lacks standing to challenge the subpoena. See Hambrick, 225 F.3d 656, at *4. "Suppression of evidence is strong medicine, not to be dispensed casually." U.S. v. Adams, 740 F.3d 40, 43 (1st Cir. 2014), cert. denied, ___ U.S. ____, 134 S. Ct. 2739 (2014). In statutory violations, the exclusionary rule is typically only triggered if the evidence sought to be excluded arises directly from violations that implicate Fourth Amendment interests. Sanchez-Llamas v. Oregon, 548 U.S. 331, 348 (2006). Historically, "[t]he cases in which the Supreme Court has

[13] The form of the administrative subpoena used by the Rhode Island State Police pursuant to § 39-2-20.1 has since been changed to comply with the certification requirement as well as the specific statutory violation that is under investigation. See Ex. 3 attached to Def's Mem.

approved a suppression remedy for statutory violations are hen's-teeth rare[.]" Adams, 740 F.3d at 43. Similarly, the Rhode Island Supreme Court has held that the "exclusionary rule is strong medicine indeed since it deprives the trier of fact in many instances of highly relevant and reliable evidence." State v. Jackson, 570 A.2d 1115, 1117 (R.I. 1990). "[T]he General Assembly of Rhode Island is quite capable of establishing an exclusionary rule when it desires to do so." Id.

This Court further notes that the administrative subpoena's directive was aimed at Verizon, not Defendant. Accordingly, this Court will not suppress otherwise admissible evidence from Defendant's trial on the grounds that it was seized unlawfully from Verizon, a party not before this Court. See Patino, 93 A.3d at 49 ('"A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his . . . Fourth Amendment rights infringed.'") (quoting Rakas, 439 U.S. at 134); see also U.S. v. Payner, 447 U.S. 727 (1980) (holding that otherwise admissible evidence should not be suppressed when it was seized, even if unlawfully, from a third party not before the court); U.S. v. Miller, 425 U.S. 435, 444 (1976) (concluding that "the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time [] the subpoena[] issue[s]").

Defendant also has no remedy under § 39-2-20.1 to exclude evidence for a statutory violation. In U.S. v. Thompson, the Eleventh Circuit held that evidence obtained allegedly in violation of a federal pen register statute was admissible because the statute does not provide a remedy for exclusion. 936 F.2d 1249, 1251-52 (11th Cir. 1991). Similar to § 39-2-20.1, the Federal Stored Communications Act (SCA) within the Electronic Communications Privacy Act

requires ISPs to disclose subscriber information to the government pursuant to an administrative subpoena, but suppression is not provided as a remedy for statutory violations. 18 U.S.C. § 2703(c)(2); see § 2707 (listing such remedies as equitable or declaratory relief, damages, and reasonable attorney's fees and other litigation costs reasonably incurred); U.S. v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014) (noting that 18 U.S.C. § 2515, the federal Wiretap Act, specifically provides for the exclusion of evidence from trial as a remedy for a statutory violation).

For all the foregoing reasons, this Court finds that Defendant lacks standing to challenge the administrative subpoena and is not entitled to the exclusionary rule under the Fourth Amendment or under § 39-2-20.1.

C

Statute

Defendant's final contention is that § 39-2-20.1 is unconstitutional inasmuch as it does not afford any opportunity for pre-compliance review, nor is it reviewed for probable cause by a neutral and detached magistrate.

The Rhode Island Supreme Court "presumes that legislative enactments are valid and constitutional." Mackie v. State, 936 A.2d 588, 595 (R.I. 2007). In reviewing a challenge to a statute's constitutionality, the Rhode Island Supreme Court exercises the "'greatest possible caution.'" Id. (quoting Cherenzia v. Lynch, 847 A.2d 818, 822 (R.I. 2004)). The Court will not hold a statute unconstitutional unless the party challenging the statute is able to "'prove beyond a reasonable doubt that the act violates a specific provision of the constitution or the United States Constitution[.]'" Id. (quoting Cherenzia, 847 A.2d at 822). Our Court has expressed the Rhode Island judiciary's "reluctance to adjudicate constitutional questions when a case is capable of decision upon other, non-constitutional grounds." State v. Lead Indus. Ass'n, Inc., 898 A.2d

1234, 1239 (R.I. 2006); Caron v. Town of N. Smithfield, 885 A.2d 1163, 1165 (R.I. 2005); In re Court Order Dated October 22, 2003, 886, A.2d 342, 350 n.7 (R.I. 2005); State v. Berberian, 80 R.I. 444, 445, 98 A.2d 270, 270-71 (1953).

In this case, Defendant must establish standing in order to challenge the constitutionality of § 39-2-20.1. See Moffett, 84 F.3d at 1293. In Moffett, the defendant admitted that he had no reasonable expectation of privacy in Amtrak's business records and did not contest the administrative subpoena under the Fourth Amendment. Id. He instead alleged, more broadly, that he had Article III case or controversy standing to challenge the statutory authority to issue the administrative subpoena. Id. The Moffett court determined that Amtrak, the entity to which the administrative subpoena was issued, could have had standing to make defendant's argument, but instead it complied. Id. The Moffett court held that in order for the defendant to have standing to challenge the constitutionality of the statute, he needed to have demonstrated "not only that he suffered actual personal injury traceable to the challenged actions but that he [was] in the zone of interest the statute is meant to protect." Id.; see also MacDonald, 710 F.3d at 162 (holding that "[a] party has standing to challenge the constitutionality of a statute only insofar as it has an adverse impact on his own rights"). In its standing analysis, the Moffett court analogized to cases in which a defendant challenged the constitutionality of a knock-and-announce statute. Id. For instance, in such cases, a defendant lacks standing to challenge a knock-and-announce statute when the defendant did not live in the house searched. Id.

Here, this Court has already determined that Defendant has no reasonable expectation of privacy in the subscriber information obtained from Verizon in response to the administrative subpoena. Accordingly, Defendant has failed to show not only that he suffered actual personal injury traceable to the challenged actions, but also that he was in the zone of interest that § 39-2-

20.1 is meant to protect. Instead, § 39-2-20.1(g) indicates that Verizon and ISPs are in the statute's zone of interest because the statute shields ISPs from civil liability when they strictly comply with the statute's requirements. While Defendant suggests he should have been afforded the opportunity for pre-compliance review and/or review by a neutral and detached magistrate for probable cause, it is Verizon or any other ISP that is within the zone of interest that may allege such unconstitutionality, and not Defendant.

This Court finds that Defendant lacks standing to challenge the constitutionality of § 39-2-20.1. Accordingly, because Defendant's challenge is not presently justiciable, any review by this Court of the constitutionality of the statute is hereby denied. See Lead Indus. Ass'n, Inc., 898 A.2d at 1239.

IV

Conclusion

Defendant cannot invoke Fourth Amendment protections because he failed to meet his burden to establish requisite standing to challenge the legality of the search and the administrative subpoena. He also failed to establish standing to challenge the constitutionality of § 39-2-20.1. For all the foregoing reasons, Defendant's motion to suppress is denied. Counsel shall submit an appropriate order for entry.

RHODE ISLAND SUPERIOR COURT

Decision Addendum Sheet

TITLE OF CASE:	**State of Rhode Island v. Enrique Rodriguez**
CASE NO:	**P2-2014-3011A**
COURT:	**Providence County Superior Court**
DATE DECISION FILED:	**May 30, 2017**
JUSTICE/MAGISTRATE:	**K. Rodgers, J.**

ATTORNEYS:

For Plaintiff:	**Owen Murphy, Esq.**
For Defendant:	**John E. MacDonald, Esq.** **Michael J. Zarrella, Esq.**