

No.17-6525

IN THE SUPREME COURT OF THE UNITED STATES

MARVIN T. RIDEOUT, III,
petitioner,

v.

HAROLD CLARKE,
respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO
THE FOURTH CIRCUIT COURT OF APPEALS

PETITION FOR REHEARING FOR WRIT OF CERTIORARI

Marvin T. Rideout, III
(VA state #) 1458599

Deerfield Correctional Center
23160 Deerfield Drive
Capron, VA 23829

QUESTION PRESENTED

The question before this Court is;

Is a wireless router, secured and password protected, providing internet connect·ability to devices in a citizen's private home, considered a private enclave and under the protection of the Fourth Amendment of the United States Constitution?

TABLE OF CONTENTS

Question presented.....	i
Table of Contents.....	ii
List of Parties.....	iii
Table of Authorities.....	iv
Petition for rehearing for Writ of Certiorari.....	1
Opinions Below.....	1
Jurisdiction.....	1
Statutory and Constitutional Provisions Involved.....	2
Reasons for Granting the Writ.....	4
Conclusion.....	10
Proof of Service	
Appendix	

INDEX TO APPENDICES

Judgement from the Fourth Circuit Court of Appeals.....	A
Unpublished opinion from the Fourth Circuit Court of Appeals.....	B
Memorandum order from the U.S. District Court.....	C
Order from the U.S. District Court.....	D
Results of Forensic Computer Investigation.....	E
Affidavit from Rideout to the U.S. District Court.....	F

LIST OF PARTIES

Marvin T. Rideout, III - petitioner
(VA state #) 1458599
[NTC Pro se]

Deerfield Correctional Center
23160 Deerfield Drive
Capron, VA 23829

v.

Harold Clarke - respondent

Mr Mathew R McGuire
[NTC Government]
Office of the Attorney General
Of Virginia
202 North 9th Street
Richmond, VA 23219

TABLE OF AUTHORITIES

Cases

Lewis v. United States, 385 U.S. 206, 87 S. Ct. 424, 427, 17 L. Ed. 2d 312;.....	5
Rios v. United States 364 U.S. 253, 80 S. Ct. 1431 4L. Ed. 2d (1968).....	5
Murphy v. Waterfront Comm'n, 378 U.S., at 55, 84 S. Ct., at 1597.....	7
Smith v. Maryland, 442 U.S. 735, 740, 99 S. Ct. 2577 61 L. Ed. 22(1979).....	7
Katz v. United States 389, U.S., 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).....	7
Olmstead v. United States 277 U.S. 438,435, 48 S. Ct. 564,575, 72 L. Ed. 944 (1928)	9

Statues

28 USC § 2254.....	8
--------------------	---

**IN THE
SUPREME COURT OF THE UNITED STATES**

PETITION FOR REHEARING FOR WRIT OF CERTIORARI

The petitioner, Marvin Rideout, III, respectfully prays that a rehearing is granted toward the petition for Writ of Certiorari. The petitioner became aware of erroneous data in the original petition submitted to the court in October of 2017, and filed a Motion to Amend on December 6, 2017. It is the belief that the petitioners petition was denied in accordance to Rule 14 of the Court. For this reason a corrected petition is being submitted with the direct question regarding the protection of the 4th Amendment of the U.S. Constitution.

The petitioner, Marvin Rideout, III, respectfully prays that a Writ of Certiorari, issue to review the judgment and opinion that the fourth Circuit Court of Appeals rendered in these proceedings on September 8, 2017, case # 17-6382

OPINIONS BELOW

The Fourth Circuit court of Appeals dismissed Rideout's appeal to the decision made by the District Court, citing a failure to demonstrate a substantial showing of the denial of a constitutional right. The Fourth Circuit Court of Appeals denied Rideout's motion for a certificate of appealability, denied leave to proceed in forma pauperis, and dismissed the appeal on September 8, 2017.

JURISDICTION

The original opinion to the Fourth Circuit Court of Appeals was entered on September 2, 2017. This opinion is unpublished per curiam opinion.

STATUTORY AND CONSTITUTIONAL PROVISIONS INVOLVED

UNITED STATES CONSTITUTION AMENDMENT IV

The right of the people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or thing to be seized.

28 U.S.C. §2254

(a) The Supreme Court, a Justice thereof, a circuit judge, or a district court shall entertain an application for a writ of habeas corpus in behalf of a person in custody pursuant to the judgement of a State court only on the ground that he is in custody in violation of the Constitution or laws or treaties on the United States.

(d) An application for a writ of habeas corpus on behalf of a person in custody pursuant to the judgement of a State court shall not be granted with respect to any claim that was adjudicated in the merits in State court proceedings unless the adjudications of the claim –

(1) resulted in a decision that was contrary to, or involved an unreasonable application of, clearly established Federal law, as determined by the Supreme Court of the United States, or

(2) Resulted in a decision that was based on an unreasonable determination of the facts in light of the evidence presented in the State court proceeding.

(2) If the applicant had failed to develop the factual basis of a claim in State court proceedings, the court shall not hold as evidentiary hearing on the claim unless the applicant shows that ---

(A) the claim relies on-

(i) a new rule of constitutional law, made retroactive to cases on collateral review by the Supreme Court, that was previously unavailable, or

(ii) a factual predicate that could not have been previously discovered through the exercise of due diligence; and

(B) The facts underlying the claim would be sufficient to establish be clear and convincing evidence that but for constitutional error, no reasonable fact finder would have found the applicant guilty of the underlying offense.

Reasons for Granting the Writ

On September 2, 2011, Sgt. Anders of the Bedford County police department, armed with an Internet Protocol (IP) address,¹ directed his software to connect with the address. Once his computer had made a connection, he directed his software to begin downloading files from a computer at the remote location. Due to the nature to the source providing the IP address, Sgt. Anders believed he would discover evidence of a particular crime. For three consecutive days, ending on September 4, 2011, Sgt. Anders connected his computer to the computer found at the remote location and downloaded multiple files. This type of connection is referred to as a peer-to-peer (P2P). Public accessible domains or websites were not involved, hence P2P. Sgt. Anders did not have a warrant to search or seize property found at IP address 174.66.3.142. After gaining several files, Sgt. Anders obtained an administrative warrant in order to force the internet provider, Cox Communications of Hampton Roads, to divulge the name and address associated with the IP. In December of 2011, Sgt. Anders, along with law enforcement from New Kent County Virginia, obtained a warrant to search and seize items of a particular nature from the residence belonging to the IP address; 7920 North Courthouse Road, New Kent, Virginia.

¹ An internet protocol address (IP), is a unique number assigned by a internet provider and to a modem and/or router at the customers location. An IP is unique and similar to a telephone number. One address is often used by multiple devices.

Sgt. Anders never witnessed Rideout commit a crime, or had any first hand knowledge of a crime, or testimony from a witness to a crime, or had any direct communication with Rideout prior to his first “fishing expedition” into Rideout’s personnel secured network..²

Rideout was convicted in large part by the belief presented by the prosecution that the computer was the front door to his network with no security prior to accessing the computer and because this computer had file sharing software installed, Shareaza, ³, this front door was wide open for all to see, thus precluding the need for a search warrant prior to the intrusion.

What a person knowingly expresses to the public, even in his own home or office is not a subject of Fourth Amendment protection, Lewis v. United States, 385 U.S. 206, 87 S. Ct. 424, 427, 17 L. Ed. 2d 312; But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. [389 U.S. 352] Rios v. United States 364 U.S. 253, 80 S. Ct. 1431 4L. Ed. 2d (1968)

Rideout researched wireless routers prior to purchase and based on statements made by D-Link Systems, Inc., Rideout purchased and installed a D-link wireless router with a factory installed firewall. This firewall required all devices to

² Network,, a group of computers and internet ready devices connected by wires or wireless (Wi-Fi) for the purpose of sharing information, devices, or an internet connection. A network’s activity and access is controlled by a router.

³ Shareaza, software that enables users to share files from one user to another, commonly referred to as peer to peer (P2P).

use a password type recognition and operated independently of any computer or device in the network. This router and firewall was operating at the time Sgt. Anders intruded into Rideout's private network. How Sgt. Anders was able to circumvent this security is unknown to Rideout; however, simply because Sgt. Anders was able to enter the network, does not indicate that vulnerabilities ⁴, in the router's software were not exploited.

Rideout has always contended that the D-link router was the actual front door to his network and this door was closed. To use the vernacular of the trial court prosecutor, Rideout's computer was likened to a bedroom door within the house. By DuVal's, ⁵ agreeing with the prosecutor that the computer was the front door and ignoring the significant role the router played in protecting Rideout and his family's constitutional right as provided by the Fourth Amendment, DuVal was ineffective in his role as defense counsel.

DuVal asked the circuit court to provide for a computer expert to research Rideout's statement that he was not sharing any files because of the firewall/router and settings on his laptop. DuVal enlisted the aid of Mr. Eric V. Myers.

⁴ **"Vulnerabilities found in D-link routers"**, In January 2010, it was reported that HNAP vulnerabilities had been found on routers and was criticized for apparently failing to resolve these problems nor informing the consumers: Infoworld

⁵ **Todd DuVal, esq.**, court appointed counsel for Rideout in the Circuit Court.

In Myer's forensic report, ⁶, he stated that; "When I requested the settings from Mr. Rideout's router, I was informed by Sgt. Anders at SOVA ICAC that they did not seize the router and that it was left at the residence because it was providing IP telephone service for his wife who was recovering from surgery at the time. " Myer's report makes it clear that DuVal knew of Rideout's claim of a secured home network; due to fact, that Myer's received direction to examine the firewall on the router. 50% of the investigation was not performed, thus heavily prejudicing Rideout's defense "to a private enclave where he may lead to a private life" Murphy v. Waterfront Comm'n, 378 U.S., at 55, 84 S. Ct., at 1597, and crippling his chance for a fair trial

A Fourth Amendment search occurs when "the person invoking its protection can claim a 'justifiable', or 'reasonable', or 'legitimate expectation of privacy' that has been invaded by government action" Smith v. Maryland, 442 U.S. 735, 740, 99 S. Ct. 2577 61 L. Ed. 22(1979). The classic analysis of this rule comes from Justice Harlon, who explained that there are two components to a reasonable expectation of privacy, "First that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as 'reasonable'" Katz v. United States 389, U.S., 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

⁶ Forensic report,, in full appears in appendix E of this Motion

5. The Federal Trade Commission ⁸ is suing D-link Systems, Inc. For misleading consumers to believe their machines had no vulnerabilities and presenting an expectation of privacy

Rideout's privacy was intruded upon.

It is "immaterial that the intrusion was in aid of law enforcement.

Experience should teach us to be most on guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding." Olmstead v. United States 277 U.S. 438,435, 48 S. Ct. 564,575, 72 L. Ed. 944 (1928)

It benefitted Sgt. Anders when he directed his software to invade a private home for the sole purpose to search for the presence to a crime that he held no proof of or testimony to.

⁸ **Federal Trade Commission (FTC)**, "The FTC sued hardware maker D-link Systems, Inc., in January, accusing it of falsely advertising that its machines were secure despite several vulnerabilities."; giving rise to society's expectation of privacy; Wall Street Journal, March 21, 2017.

CONCLUSION

For these reasons, a writ of certiorari should be issued to review the judgement and opinion of the Fourth Circuit Court of Appeal in not addressing a clear violation of the 4th amendment of the U.S. Constitution, granting citizen's the right to live a private life in their homes.

Respectfully submitted,

A handwritten signature in cursive script, reading "Marvin T. Rideout, III". The signature is written in dark ink and is positioned below the phrase "Respectfully submitted,".

Marvin T. Rideout, III
#1458599 – DOC ID
Deerfield Correctional Center
21360 Deerfield Drive
Capron, VA 23829

Marvin T. Rideout, III

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 17-6382
(3:16-cv-00190-MHL-RCY)

MARVIN RIDEOUT

Petitioner – Appellant

v.

HAROLD CLARKE, D.O.C.

Respondent – Appellee

JUDGMENT

In accordance with the decision of this court, a certificate of appealability is denied and the appeal is dismissed.

This judgement shall take effect upon issuance of this court's mandate in accordance with Fed. R. App. P. 41.

/s/ PATRICIA S. CONNOR, CLERK

UNPUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 17-6382

MARVIN RIDEOUT

Petitioner – Appellant

v.

HAROLD CLARKE, D.O.C.

Respondent – Appellee

Appeal from the United States District Court for the Eastern District of Virginia, at
Richmond. M. Hannah Lauck, District Judge. (3:16-cv-00190-MHL-RCY)

Submitted: August 30, 2017

Decided: September 8, 2017

Before WILKINSON, NIEMEYER, and FLOYD, Circuit Judges.

Dismissed by unpublished per curiam opinion.

Marvin Rideout, Appellant Pro Se. Rosemary Virginia Bourne, OFFICE OF THE
ATTORNEY GENERAL OF VIRGINIA, Richmond, Virginia, for Appellee.

Unpublished opinions are not binding precedent in this circuit.

PER CURIAM:

Marvin Rideout seeks to appeal the district court's order accepting the recommendation of the magistrate judge and denying relief on his 28 U.S.C. § 2254 (2012) petition. The order is not appealable unless a circuit justice or judge issues a certificate of appealability. 28 U.S.C. § 2254 (c)(1)(A) (2012). A certificate of appealability will not issue absent "a substantial showing of the denial of a constitutional right" 28 U.S.C. § 2254 (c)(2) (2012). When the district court denies relief on the merits, a prisoner satisfies this standard by demonstrating that reasonable jurists would find that the district court's assessment of the constitutional claims is debatable or wrong. *Slack v. McDaniel*, 529 U.S. 473, 484 (2000); see *Miller-El v. Cockrell*, 537 U.S. 322, 336-38 (2003). When the district court denies relief on procedural ruling is debatable, and that the petition states a debatable claim of the denial of a constitutional right. *Slack*, 529 U.S. at 383-85.

We have independently reviewed the record and conclude that Rideout has not the requisite showing. Accordingly, we deny Rideout's motion for a certificate of appealability, deny leave to proceed in forma pauperis, and dismiss the appeal. We dispense with oral argument because the facts and legal contentions are adequately presented in the materials before this court and argument would not aid the decisional process.

DISMISSED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

MARVIN RIDEOUT,

Petitioner,

v.

Civil Action No. 3:16CV190

HAROLD CLARKE,

Respondent.

MEMORANDUM ORDER

By Memorandum Opinion and Order entered on February 28, 2017, the Court denied Petitioner's 28 U.S.C. § 2254 Petition and denied a certificate of appealability ("COA"). *Rideout v Clarke*, No. 3:16CV190, 2017 WL 811492, at *9 (E.D. Va. Feb. 28, 2017). Petitioner has filed and Application for Certificate of Appealability. (ECF No.33) If Petitioner wishes to challenge this Court's denial of a COA, he should file such a challenge with the United States Court of Appeals for the Fourth Circuit. Local Rule for the United States Court of Appeals for the Fourth Circuit 22(a)(1)(A) contemplates that review of a district court's denial of a COA should be directed to the Fourth Circuit not the district court. 4th Cir. Loc R. 22(a)(1)(A) (when "the district court has not granted a [COA]....appellant may submit a request for a [COA] with the Court of Appeals specifying the issues on which the appellant seeks authorization to appeal and giving a statement of the reasons why a certificate should be issued"). Accordingly, Petitioner's Application for Certificate of Appealability (ECF No. 33) is DENIED.

The Clerk is DIRECTED to send a copy of this "Order to Petitioner and the Clerk for the United States Court of Appeals for the Fourth Circuit.

It is so ORDERED.

/s/ Roderick C. Young
United States Magistrate Judge

Date: April 7, 2017
Richmond, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

MARVIN RIDEOUT,

Petitioner,

v.

Civil Action No. 3:16CV190

HAROLD CLARKE,

Respondent.

ORDER

In accordance with the accompanying Memorandum Opinion, It is hereby ORDERED that:

1. The Report and Recommendation (ECF No. 18) is ACCEPTED and ADOPTED;
2. Respondent's Motion to Dismiss (ECF No. 5) is GRANTED;
3. Rideout's § 2254 Petition (ECF No. 1) and Amended § 2254 Petition (ECF No. 22-1) are DENIED;
4. Rideout's original Motion for Leave (ECF No. 14) is DENIED;
5. Rideout's Motion for Leave (ECF No. 21) and Motion to Amend (ECF No. 22) are GRANTED;
6. Rideout's claims and the action are DISMISSED; and,
7. A certificate of appealability is DENIED.

Should Rideout desire to appeal, a written notice of appeal must be filed with the Clerk of the Court within thirty (30) days of the date of entry hereof. Failure to file a notice of appeal within that period may result in the loss of the right to appeal.

The Clerk is DIRECTED to send the Memorandum Opinion and Order to Becton and counsel of record..

It is so ORDERED.

/s/ Ms. Hannah Lauck
United States District Judge

Date: February 28, 2017
Richmond, Virginia

Results of Forensic Computer Investigation

In the case of

Commonwealth of Virginia vs. Marvin T. Rideout, III

Date: July 26, 2012
Investigator Eric V. Myer

This report includes the results of my investigation of select computer files and registry entries from the computer of Marvin T. Rideout, III. The data was provided by the Southern Virginia Internet Crimes Against Children (SOVA ICAC) task force forensic investigator, Kevin Davis from an image made of Mr. Rideout's computer after its seizure on December 16, 2011.

Conclusion:

Mr. Rideout says that he disabled sharing because he didn't want his personal files shared. It appears that he removed from the sharing library the default folders that Shareaza creates and automatically shares upon installation; however, I have determined that at some point he changed the location where his completed downloads were stored to the folder the contained his pornography catalog. The action of changing the location in the settings automatically and with notification adds the folder to the sharing library, along with everything it contains.

I conclude the Mr. Rideout appears to have made the effort to prevent the sharing of files, but was thwarted in that effort by the operation of the program. P2P software is written with sharing in mind and it's anathema to the P2P community when users want to take and not give. The software wants to make your files available to others and it's often difficult to prevent the practice. Even if he thought he was otherwise protected behind his firewall/router, Gnutella has a way around push requests.

Background:

Libray1.dat: This file contains the list of files of folders and files shared through Shareaza. In looking through this file, I see that Mr. Rideout was sharing several folders and their contents. I recognized one of these folders as the location where investigator Davis showed me that Mr. Rideout was cataloging his pornography. Shareaza allows the user to disable sharing on a per-file basis, but for 40 or so files whose entries I viewed, sharing was enabled.

Firewall Routers and firewalls are notorious for interfering with P2P traffic, especially in preventing external peers from downloading files from a peer behind the firewall/router. Even though files are listed for sharing, trying to retrieve the file would fail as the traffic was blocked by the firewall. To prevent this problem, a port must be opened in the firewall and the traffic forwarded to the computer hosting the P2P software. When I requested the settings from Mr. Rideout's router, I was informed by Sgt. Anders at SOVA ICAC that they did not seize the router and that it was left at the residence because it was providing IP telephone service for his wife who was recovering from surgery at the time. Therefore, I cannot determine if Mr. Rideout had opened the Shareaza port on his router to facilitate uploads of the files he was sharing. He would have had to have done this manually because the "Enable UPnP (Universal Plug and Play) connection device setup" setting in Shareaza was turned off, meaning that the software would not have tried to open the port automatically.

Gnutella Push: The designer of the Gnutella network, recognizing the problem of peers trying to share files behind firewalls and uploads failing due to closed ports, designed a mechanism called a "push request" whereby the external peer can instruct the sharing peer to push (send) the file directly to it, thereby circumventing any firewalls or routers preventing direct connections. Shareaza does support push requests and although they are less reliable than making direct (pull) requests, they do allow sharing from behind a firewall. Even if Mr. Rideout had not opened the Shareaza port on his router,, it is possible that his shared files could have been uploaded via a push request.

Unfortunately, there is no way for me to know if this did or did not happen.

"[I] Can accept incoming connections" setting: Shareaza has a setting called "[I] Can accept incoming connections", which defaults to "auto". According to the registry entries from Mr. Rideout's computer, this file was set to "auto" on his machine. The purpose of this setting (according to the documentation on SourceForge, the repository for the open source code for Shareaza) is to inform Shareaza of the presence or absence of a firewall. In fact, internally this setting is called "firewallState". The program automatically tries to determine if the peer is firewalled (prevented from accepting upload requests) and if so, will notify the user so that they can take action, if desired.

The user can effectively force Shareaza to believe that it is firewalled to changing the setting to "no" – saying that "I CANNOT accept incoming connections" in that case the user wants to prevent pull sharing (maybe due to ISP issues, etc.) Conversely, if Shareaza has determined that it is firewalled, the user can override that determination by changing the setting to "yes" – affirming that "I CAN accept incoming connections". Leaving the setting on "auto" allows Shareaza to use its own results and act accordingly.

One important note is that this setting does not imply that uploading of files is PREVENTED I.E., it is not a quick "shut off sharing" button. Sharing can still occur via push requests, saw noted above. As in all firewalled cases, real or otherwise, sharing is hampered, but not prevented.

Other "sharing" settings: The only settings on Mr. Rideout's computer related to sharing that I see having been turned off are "Share NEW partial downloads" and "Share preview files", neither on would prevent sharing of completed files.

The "Results of Forensic Computer Investigation" report was retyped to conform to Rule 34:

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**

Marvin Rideout,
Petitioner,

v.

CIVIL ACTION NO:3:16cv190

Harold Clarke,
Respondent

AFFIDAVIT

1. I AM THE UNDERSIGNED AFFIANT.
2. I BASE THESE STATEMENTS OF THE BEST OF MY KNOWLEDGE AND BELIEF.
3. THE AFFIANT STATES THE FOLLOWING:

On December 16, 2011, at approximately 6:45 am, Sgt. Anders and Det. McLaughlin appeared at my residence. They served me with a search warrant. I read the search warrant. I allowed Sgt. Anders and Det. McLaughlin to enter my residence at 7920 North Courthouse Rd., New Kent, Virginia. Sgt. Anders was carrying a bag. Up to this point there was no dialogue between myself and the police officers. At no time did I make the statement: "I've been waiting for you all to come." I never knew the police accused me of making such a statement until I saw it in the appellate court's ruling.

I was asked to wait outside initially. However, after some thirty minutes, I was escorted into my residence by Det. McLaughlin as he informed me that he needed to know where my computer was. I went with Det. McLaughlin into my bedroom and McLaughlin picked up my laptop. We went into the dining room and handed my laptop to Sgt. Anders who was seated at my dining room table. I observed Sgt. Anders set my laptop next to his on the table. He then removed cables from the bag

that he was carrying and connected the two laptops together by this cable. He then entered a password into his laptop and operated both computers using his computer's keyboard only. I realized that the cable he was using to connect the two computers was a firewire. This firewire allows for a faster and more direct connection. I was standing approximately two feet from Sgt. Anders, while Det. McLaughlin stood to my left checking my cell phone. Sgt. Anders connected to my computer for about forty minutes. I informed Mr. Duval of Sgt Anders actions prior to going to trial.

I DECLARE UNDER PENALTY OF PERJURY THAT THE FOREGOING IS TRUE
AND CORRECT.


Signature of Affiant

This Affidavit report was retyped to conform to Rule 34: