COURT OF APPEALS OF VIRGINIA

Present: Judges Humphreys, Russell and Senior Judge Bumgardner
Argued at Norfolk, Virginia

PUBLISHED

MATTHEW JOHN STICKLE

v. Record No. 0660-16-1

COMMONWEALTH OF VIRGINIA

OPINION BY
JUDGE ROBERT J. HUMPHREYS
DECEMBER 27, 2017

FROM THE CIRCUIT COURT OF THE CITY OF WILLIAMSBURG AND
COUNTY OF JAMES CITY
Michael E. McGinty, Judge

Patricia Palmer Nagel for appellant.

John I. Jones, IV, Assistant Attorney General (Mark R. Herring, Attorney General, on brief), for appellee.

Matthew John Stickle ("Stickle") appeals his December 16, 2015 conviction in the Circuit Court of the City of Williamsburg and County of James City (the "circuit court") on three counts of possession of child pornography, first and second or subsequent offenses, and twenty-two counts of possession of child pornography with intent to distribute.

I. Background

"In accordance with established principles of appellate review, we state the facts in the light most favorable to the Commonwealth, the prevailing party in the [circuit] court. We also accord the Commonwealth the benefit of all inferences fairly deducible from the evidence." Muhammad v. Commonwealth, 269 Va. 451, 479, 619 S.E.2d 16, 31 (2005).

So viewed, the evidence shows that on September 3, 2013, Lieutenant Scott Little ("Little"), a district coordinator of the Southern Virginia Internet Crimes Against Children Task Force, took part in an undercover investigation into what is known as peer-to-peer ("P2P")

distribution of child pornography over the internet. Little testified regarding his substantive role in the investigation of Stickle and also testified without objection as an expert in the field of digital forensics, in particular "as to the investigation of child exploitation offenses."

Although the record reflects that much of Little's testimony is somewhat technical, the specifics are important to the legal analysis in this case and are essentially as follows:

What is generically referred to as "the internet" is a cooperatively managed global network of smaller interconnected networks. Each internet site, whether such site is hosted on a computer server or a single specific computer, is associated with a unique internet protocol ("IP") address. Likewise, each device accessing the internet, such as computers, tablets, modems, routers, and smart phones, necessarily also is assigned a unique IP address to facilitate two-way communication with other devices and locations on the internet.[1] The most common method of accessing internet sites is through a software application known as a "browser," such as Microsoft's Internet Explorer or Apple's Safari. Browsers can access that portion of the internet known as the Worldwide Web or simply "the web," which is the roughly fifteen percent of the internet sites that have been assigned domain names and indexed by Google and other search engines.[2] Using a browser to access a site on the Worldwide Web requires that the link be

[1] An IP address is a unique 128 bit number assigned by the Domain Name Server ("DNS") of an internet service provider to each specific customer. IP addresses of individual devices within that customer's premises are assigned and maintained by a DNS in a device called a router that creates a subnetwork within the premises based upon the IP address assigned by the internet service provider. Overall worldwide management of IP addresses and associated domain names is the responsibility of the Internet Corporation for Assigned Names and Numbers (ICANN).

[2] The web is defined as a collection of links to the registered domain names of internet locations or "web pages" created using HTML (Hypertext Markup Language) thereby enabling them to be indexed by search engines and displayed in a browser. The remainder and vast majority of internet sites, known as the "deep web," consists of unindexed, non-HTML locations, resources, and data that are encrypted, protected by a password, behind a paywall or otherwise beyond the reach of search engines and includes such things as email addresses, private networks

routed through one or more DNS servers located throughout the world that maintain a current database of IP addresses and their associated domain names and direct internet traffic to the appropriate IP address.[3]

A less common, but nevertheless widely available and frequently used method of reaching a specific IP address is through a direct link that is not relayed through a routing DNS. Using specialized but readily obtainable software designed for the purpose, a direct, encrypted "peer-to-peer" or "P2P" link can be established between a user's computer and a specific folder or file on any linked computer—provided that the owner of the destination computer is using similar P2P software and has allowed specific access to such folder or file location.

In short, P2P networks use locally installed software called a "client" which allows users to share computer files of their choice directly with other similarly equipped users (a "peer") and without any intermediary routing. Files which a user intends to share are kept in a specific folder designated as sharable by the software client. While there is nothing inherently illegal about the use of peer-to-peer file sharing, P2P software is often used to share files in violation of copyright and other intellectual property laws and to facilitate communications regarding various types of

---

and on-line banking sites. A small, encrypted subset of the deep web known as the "dark web" consists of peer-to-peer networks such as Tor, Freenet or, as in this case, ARES, and requires specific software, hardware configurations or authorization to access. See generally, Andy Greenberg, Hacker Lexicon: What Is the Dark Web?, Wired Magazine, November 19, 2014.

[3] By way of example, www.vacourts.gov is the domain name registered with ICANN for the internet site hosting the on-line presence of the judicial department of the Commonwealth of Virginia. Entering www.vacourts.gov into a web browser will cause it to contact a DNS, lookup the IP address assigned to the domain name www.vacourts.gov which will return the associated IP address 208.210.219.101 and then link to that IP address and display the web page located there.

criminal activity.[4] Because P2P locations in the dark web are invisible to indexing and search engines such as Google, specialized software is required to access each separate P2P network.

Little was focusing his investigative attention on the ARES P2P network, which is often used to exchange child pornography. Testifying as an expert, Little explained how peer-to-peer networks are used in the context of the exchange of child pornography.

In a P2P network generally, users place any files they wish to share with others in a specific "shared" folder. P2P clients like ARES globally search all shared folders in the P2P network for any specified files. If found, the client then connects directly to all "peers," i.e. computers with shared folders that host the particular file being sought, and different pieces of the file are then downloaded from multiple peers and reassembled into a new whole copy which is then saved to the user's shared folder.[5]

Specifically, with respect to the use of ARES, Little testified that file source IP addresses are always collected by a P2P client, but in the stock version of ARES, they are not normally displayed to the user. An ARES user enters the name of any file sought into the ARES client. As with other P2P software, ARES then locates multiple IP addresses of computers hosting copies of the requested file, verifies that all copies available are identical to each other, then downloads separate pieces of the file from the many different copies found across the internet, reassembles the pieces into a new copy and, after verifying that the newly assembled copy is identical to the those from which it was assembled, saves the new file copy to the user's computer.

[4] Under the "Sony standard" articulated by the Supreme Court in Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984), a device does not constitute contributory copyright infringement so long as the device is capable of "substantial non-infringing uses."

[5] Apparently, this is done to preserve the anonymity of any single peer.

Little used a specialized version of the ARES client designed specifically for law enforcement ("ARES Round Up"). ARES Round Up, has been modified from its stock configuration in two ways. First, ARES Round Up forces the client to download a shared file from a single location instead of doing so piecemeal from multiple locations and then assembling the pieces into a whole copy of the sought-after file. The second law enforcement modification to the ARES client allows law enforcement users to view the actual IP address of the target computer containing the file location of a P2P shared file.

Little input the names of specific child pornographic images encrypted and verified through the Secure Hash Algorithm ("SHA")[6] and commonly exchanged by those interested in child pornography into ARES Round Up and instructed the ARES Round UP client to search the ARES network for matches. This process allows the verified SHA values to be used to search for identical copies of known files. Little had enabled ARES Round Up to constantly search the P2P network for matches with the SHA values of known child pornography image and video files. One of these SHA values matched to a shared folder location on a computer indicating an IP address within the task force's geographic area.

Little obtained a subpoena and served the internet service provider to obtain the physical address associated with that IP address - the shared home of Stickle and his fiancée Margaret Mallory ("Mallory"). Stickle had been living at this address since moving from New York to live with Mallory in August of 2013. Little obtained a search warrant for this address and executed it on December 27, 2013. Pursuant to the warrant, police seized two laptop computers. Mallory identified one of the laptops as belonging to her, the other she identified as Stickle's.

[6] The Secure Hash Algorithm compares two files at the basic binary level and calculates a unique checksum for the authenticity of digital data to ensure the integrity of a file. In effect, it is a digital signature that indicates if a file has been modified from its original form.

Mallory initially told Little that she had no access to Stickle's device, but later amended her statement to admit she had used Stickle's computer on a few occasions.

Police conducted a forensic analysis on the laptops. Inside a password-protected user account titled "Matt" on Stickle's laptop, police found both images and videos of child pornography and the ARES client, as well as personal and family photos relating to Stickle. The ARES client's shared folder contained an "extensive" library of child and adult pornography. Some files dated back to 2010, three years before the device was seized. Little was also able to forensically retrieve the search history of the ARES client, indicating which types of files the user had been looking to obtain. It included explicit sexual terms referencing children. The in-client ARES chat function on Stickle's computer had been set to indicate to others that the user was a 14-year-old male. In addition, there were three child pornography videos featuring Stickle himself in another folder labelled "X." The X folder was located near other folders which were personally relevant to Stickle, specifically one regarding a relative's baptism. The three video files located in the X folder portrayed Stickle performing sexual acts on a prepubescent eight-to-ten-year-old male.

When interviewed by police, Stickle denied knowledge of any child pornography on his computer and stated that he had had several roommates prior to moving to Virginia to live with Mallory. One of these roommates testified at trial that he had used Stickle's computer when they lived together. He also testified that he had seen another roommate use Stickle's computer. He did not testify that he had used ARES or placed any files on Stickle's computer or seen any other roommate do so.

A grand jury indicted Stickle on twenty-two counts of possession with intent to distribute child pornography, first and second or subsequent offenses, and three counts of manufacture of child pornography, first and second or subsequent offenses. The Commonwealth dropped the

manufacture of child pornography charges when it was discovered that the videos had been created in New York, Stickle's residence before he moved to Virginia to live with Mallory. Stickle was tried on the remaining twenty-two charges in June of 2014. This trial ended in a mistrial. A grand jury subsequently indicted Stickle for three additional counts of possession of child pornography, first and second or subsequent offenses based upon the videos found in the X folder. The Commonwealth amended the twenty-two possession with intent to distribute child pornography indictments to first offense. Stickle was tried again by a jury on all twenty-five charges and found guilty on all counts.

II. Analysis

A. Application of the Fourth Amendment

Stickle sought suppression of the evidence on the grounds that Little's use of ARES Round Up to download child pornography from a computer in Stickle's home violated his Fourth Amendment rights. "Since the constitutionality of a search and seizure under the Fourth Amendment involves questions of law and fact, we give deference to the factual findings of the trial court but independently decide whether, under the applicable law, the manner in which the challenged evidence was obtained satisfies constitutional requirements." Jackson v. Commonwealth, 267 Va. 666, 672, 594 S.E.2d 595, 598 (2004).

For the past fifty years, "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." Smith v. Maryland, 442 U.S. 735, 740 (1979) (internal citations omitted). Justice Harlan's concurrence in Katz v. United States, 389 U.S. 347 (1967), proposed a two-part test for evaluating the expectation of privacy. Formally adopted in Smith v. Maryland, the Katz test first asks "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy." Smith, 442 U.S. at 740

(quoting Katz, 389 U.S. at 361). Second, it asks "whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as "reasonable."'" Id.

This Court recently applied the Katz test to a case nearly identical to Stickle's. In Rideout v. Commonwealth, 62 Va. App. 779, 753 S.E.2d 595 (2014), the same law enforcement task force that tracked Stickle used a modified version of a different P2P client (Shareaza) to download child pornography from Rideout. He sought suppression of this pornographic evidence on the theory that his failed attempt to prevent the P2P client from sharing his files established a reasonable expectation of privacy. We held in Rideout that "by simply installing file-sharing software onto his computer, appellant has 'failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable.'" Id. at 789, 753 S.E.2d at 600 (internal citation omitted).

Stickle argues the inverse of Rideout. Instead of claiming that he attempted to limit sharing, Stickle stresses both the fact that file sharing is enabled by default in ARES and that he was unaware the ARES client was on his computer or that the client was being used to download child pornography. By denying knowledge of the software, Stickle attempts to circumvent the "reasonable expectation of privacy" Katz test and tie Little's "search" to the earlier, more fundamental, property-based foundation of Fourth Amendment application resurrected by the Supreme Court in the wake of United States v. Jones, 565 U.S. 400 (2012). Though Katz originally broke with the previous property-based application of Fourth Amendment protection by declaring that the Fourth Amendment protects "protects people, not places," Katz, 389 U.S. at 351, the Supreme Court in Jones revived and reinforced the pre-Katz concept of a property interest component to Fourth Amendment protection as a backstop to a privacy interest. However, Stickle's legal argument necessarily depends upon both a misunderstanding of the

technology involved in this case and complete disregard for our standard of review. Stickle interweaves three specific Fourth Amendment arguments which we separate below for clarity.

Stickle first claims that Little, using ARES Round Up software, "entered the curtilage and threshold of [his] home without a warrant to search for evidence of probable cause of a crime." Stickle cites Florida v. Jardines, 569 U.S. 1 (2013), where the Supreme Court reversed a drug conviction because police had used a drug-sniffing dog on the defendant's curtilage. The Supreme Court held this was an unreasonable search, stating "[t]he Katz reasonable-expectations test 'has been *added to*, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment, and so is unnecessary to consider when the government gains evidence by physically intruding on constitutionally protected areas." Jardines, 569 U.S. at 11 (citing Jones, 565 U.S. at 409). Stickle claims Little "actually crossed the threshold of the house to reach the modem [sic] in order to find probable cause to obtain a search warrant." Analogizing to Jardines, Stickle argues

> [j]ust as the officer's use of a drug-sniffing dog constituted a warrantless search of the curtilage of the home, Little's use of the cable lines to the house to search the inside of the home constitutes a warrantless search of the curtilage of the home in this case. In fact, Little would not have been able to search the modem and router without use of the cable lines to the house to access these items inside of the house. Therefore, Little's actions constitute a warrantless search of the curtilage of Stickle's home.

The curtilage is a well-established common law concept describing the area immediately surrounding one's house, as defined by "its relationship to the residence and its use by its occupants." Foley v. Commonwealth, 63 Va. App. 186, 195, 755 S.E.2d 473, 478 (2014). The term "curtilage," as it is used in the legal context, "is historically understood to refer to an extension of the home that is so intertwined with the home that the law must provide it the same protection as the home itself." Id. It does not include the interior of the home which is specifically protected from warrantless intrusion by the text of the Fourth Amendment itself.

While the lines carrying internet service to Stickle's home may indeed run through his curtilage, we need not engage in an esoteric determination and analysis of the precise physical location where the bits and bytes constituting digital images of child pornography were obtained because Little's actions with respect to his use of P2P software in no way constituted a search of the cables, curtilage, computer or any other location protected by Stickle's Fourth Amendment rights. To be clear, any "search" essentially involves prying into a private place. See, e.g., United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."). However, it is well-settled that viewing items deliberately exposed to public view does not constitute a search and in any event, consensual searches and seizures of items within the scope of the consent given do not implicate the Fourth Amendment. See, e.g., Coolidge v. New Hampshire, 403 U.S. 443 (1971) (generally discussing the application of the "plain view" doctrine); United States v. Williams, 41 F.3d 192, 196 (4th Cir. 1994) (holding that "[u]nder certain circumstances, the police may seize the contents of a container found in a lawfully accessed place, without a warrant, if the contents are in plain view"); United States v. Karo, 468 U.S. 705 (1984) (concluding that there was no violation of the Fourth Amendment through a beeper placed in chemical container as it was placed with consent of the then owner); United States v. Dunn, 480 U.S. 294, 307 (1987) (establishing a four-factor test for determining the extent of the curtilage, including "the steps taken by the resident to protect the area from observation by people passing by").

Here, no warrantless search of any area or seizure of any item protected by the Fourth Amendment occurred at all. When a user "searches" a P2P network, the software client is matching the search parameters to the contents of each P2P linked computer's shared folder that others, such as Stickle, chose to make publicly available. In other words, Stickle was essentially broadcasting the contents of his shared folder to the entire ARES network community in

response to outside user queries and inviting them to copy anything and everything in the folder he chose to share. Stickle's shared folder thus represents an "implicit invitation" of the type discussed in Jardines—a cultural custom, like placing a door knocker on the front door, "treated as an invitation or license to attempt an entry, justifying ingress to the home by solicitors, hawkers and peddlers of all kinds." Jardines, 569 U.S. at 8 (quoting Breard v. Alexandria, 341 U.S. 622, 626 (1951)).

Such customs are easily understood and "generally managed without incident by the Nation's Girl Scouts and trick-or-treaters." Id. Jardines ultimately held that such invitations are limited both in area and purpose, not present here, which ultimately rendered the search in Jardines unconstitutional. See id. at 9. Here, however, the invitation provided to others directly involved child pornography. To expand upon Justice Scalia's analogy from Jardines, placing a jack-o'-lantern on the porch and leaving the light on during the evening of October 31 signifies a homeowner's participation in the annual All Hallows Eve exception to parents' usual admonition to their children that they should not accept candy from strangers.

Similarly, viewing the record in the light most favorable to the Commonwealth, Stickle demonstrated his consensual participation in the file sharing community by downloading and installing the ARES client and then setting the contents of a folder as "shared" thereby exposing to public access those files in that folder he wished to share with others. Little, in effect a digital passerby, merely accepted the invitation offered by Stickle to help himself to copies of the contents of Stickle's shared folder. Therefore, we reject Stickle's argument that Little's actions constituted a trespass to his curtilage in violation of the Fourth Amendment.

Stickle next argues that ARES Round Up violated his Fourth Amendment rights because it is "sophisticated equipment" prohibited by Kyllo v. United States, 533 U.S. 27 (2001). In Kyllo the Supreme Court overturned a drug conviction where police used a thermal imaging

device to detect heat from a marijuana growing operation within a house. Kyllo held that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Id. at 40.[7] Unlike the device used in Kyllo, however, ARES Round Up is only slightly modified from the base ARES client, allowing it to connect to only one computer to download a file rather than to do so piecemeal from as many as are advertising the availability of the file, and also by allowing it to display the connected IP address to the investigating officer. These modifications, while clearly features of the software not readily available to the general public, are not of such sophistication that they represent a level of technology not available to the general public as was the case in Kyllo.

As Little testified, the modification to allow direct connection to a single user is not an unknown advancement but rather a regression in technology to earlier file sharing protocols. File sharing software between individuals has been in general public use since the advent of the original file sharing service, Napster, in 1999—much to the vexation of the music and movie industries.[8]

The second law enforcement modification simply displays the IP address of the source shared folder—data that is already captured, though not displayed, by the standard ARES client.

[7] As an aside, we observe that Kyllo also creates an endemic problem for the courts as we try to apply 18th and 19th century legal and constitutional concepts to 21st century technology. The very infrared imaging device described in Kyllo is now widely available and can be readily purchased by the general public and thus, under its own analysis, would no longer render the search in Kyllo unconstitutional.

[8] See Menn, Joseph, All the Rave: The Rise and Fall of Shawn Fanning's Napster. Crown Business, (2003).

The nature of the minor modifications present in ARES Round Up do not, in our judgment, suffice to render it a presumptively unconstitutional law enforcement tool.

Moreover, unlike in Kyllo, ARES Roundup was not used "to explore details of the home that would previously have been unknowable without physical intrusion." Rather, its modifications simply displayed the IP address of a single computer containing a copy of a file sought—information which was broadcast to everyone on the network by the ARES software on Stickle's computer.

Finally, Stickle argues that the warrant Little obtained subsequent to downloading the child pornography from Stickle's IP address "was issued based upon an unlawful and generalized search." Stickle claims that, because Little ran ARES Round Up continuously searching widely for any file being offered on the network which matched certain SHA values, his "search" violated the particularity requirement the Fourth Amendment places on warrants. Stickle specifically asserts that "Little . . . conduct[ed] a search into the curtilage of the homes and across the threshold of the homes of all of the citizens within a region, including Stickle's home, that Little decided to subject to law enforcement surveillance for criminal activity without probable cause to do so without the knowledge or consent of the citizens." (sic) This again is a misrepresentation of the technology. Little did not "[search] the modem for the IP address." Little searched the ARES network, a voluntary file-sharing community, for very specific files containing images of child pornography from users willingly sharing those specific files. As discussed above, these users, including Stickle, essentially invited anyone, including Little, to connect directly to a *specific* set of files on their computers for the purpose of making copies. We therefore conclude that no general search in violation of the Fourth Amendment occurred.

B. Joinder of Offenses

Stickle next argues that the circuit court erred by permitting him to be charged jointly for possession of the three child pornography videos located in the unshared X folder and the twenty-two child pornography still images found in the ARES shared folder. He asserts that the charges have "no connection to show a common scheme or plan, same act or transaction, or that the two sets of alleged charges are linked or connected in any way."

"The circuit court's decision to join offenses for trial is reviewed for abuse of discretion." Walker v. Commonwealth, 289 Va. 410, 415, 770 S.E.2d 197, 199 (2015) (citing Scott v. Commonwealth, 274 Va. 636, 644, 651 S.E.2d 630, 634 (2007)). An accused may be tried at one time for more than one offense "if justice does not require separate trials and (i) the offenses meet the requirements of Rule 3A:6 (b) or (ii) the accused and the Commonwealth's attorney consent thereto." Rule 3A:10(c). Rule 3A:6(b) permits joinder of multiple offenses in an indictment "if the offenses are based on the same act or transaction, or on two or more acts or transactions that are connected or constitute parts of a common scheme or plan." Rule 3A:6(b).

Our Supreme Court has held that "the terms 'common scheme' and 'common plan' are not synonymous." Scott, 274 Va. at 645, 651 S.E.2d at 635. However, neither are they mutually exclusive. Id. at 646, 651 S.E.2d at 635. Scott defined both terms for the first time. A common scheme is composed of "crimes that share features idiosyncratic in character, which permit an inference that each individual offense was committed by the same person or persons as part of a pattern of criminal activity involving certain identified crimes." Id. at 645, 651 S.E.2d at 635 (citations omitted). A common plan consists of "crimes that are related to one another for the purpose of accomplishing a particular goal." Id. at 646, 651 S.E.2d at 635 (citations omitted). Further, the Virginia Supreme Court has stated that "offenses may be considered parts of a common scheme or plan when they are 'closely connected in time, place, and means of

commission.'" Walker, 289 Va. at 416, 770 S.E.2d at 199 (quoting Satcher v. Commonwealth, 244 Va. 220, 229, 421 S.E.2d 821, 827 (1992)).

Stickle argues that, though the pornographic files were all seized on the same date, they were placed on the computer at different dates over a range of years and are thus separate crimes that are not part of a common scheme or plan. However, Stickle is being charged with *possession* of these pornographic videos and *possession* with intent to distribute the various pornographic images, both of which are, "by nature," continuing offenses. Morris v. Commonwealth, 51 Va. App. 459, 467, 658 S.E.2d 708, 712 (2008). At the moment Stickle's computer was seized he was in possession of each of the files reflected in the charges irrespective of the date they were originally placed there.

To protect defendants from being prosecuted multiple times for arbitrary divisions of offenses, the law long ago adopted the rule that "'a continuing offence . . . can be committed but once, for the purposes of indictment or prosecution.'" In re Nielsen, 131 U.S. 176, 186 (1889) (discussing multiple prosecutions for "unlawful cohabitation," another continuous offense). Stickle argues that the twenty-two possession with intent to distribute charges should be separated from the three possession charges related to the X folder, but he provides no logical resting place for his argument. Among the questions Stickle's argument implicitly raises but does not answer are: Is child pornography more easily divisible than cocaine? Should a drug dealer charged with possession of twenty-five grams of cocaine have twenty-five (or more if a smaller unit of measurement is chosen) separate trials? Should a thief be tried separately for every unit of currency or item stolen? The executive branch of government, in the form of the Commonwealth's Attorney, exclusively controls the charging decision and has wide discretion in doing so, subject only to constitutional or statutory limitations. Stickle's argument slides easily down a slippery slope which, if adopted, would serve no purpose beyond devastating judicial

efficiency. Consistent with both Rules 3A:10(c) and 3A:6(b), the offenses here are so interrelated as to constitute part of a common scheme or plan to collect and/or distribute child pornography. Therefore, we conclude that the circuit court did not abuse its discretion in allowing joinder of all the offenses for trial.

Stickle alternatively argues that, even if joinder requirements were satisfied, the three videos are so prejudicial that justice requires separate trials. He claims the videos constitute impermissible character evidence and that the circumstances surrounding their creation are factually distinct from those regarding the pornographic images in the shared folder. In weighing the prejudice of evidence against its probative value "We generally defer to trial judges . . . because they, unlike us, participate first person in the evidentiary process and acquire competencies on the subject that we can rarely duplicate merely by reading briefs and transcripts." Thomas v. Commonwealth, 44 Va. App. 741, 758, 607 S.E.2d 738, 746, adopted upon reh'g en banc, 45 Va. App. 811, 613 S.E.2d 870 (2005) (citing Dandridge v. Marshall, 267 Va. 591, 596, 594 S.E.2d 578, 581 (2004)).

Stickle relies on Hackney v. Commonwealth, 28 Va. App. 288, 504 S.E.2d 385 (1998) (*en banc*), and Long v. Commonwealth, 20 Va. App. 223, 456 S.E.2d 138 (1995), both cases where severance was ultimately required where other crimes evidence was introduced to show possession of a firearm by a convicted felon. The precedent set by these cases is stark but narrow, they are limited to this unfortunately common scenario: "a trial court must sever a charge of possession of a firearm by a convicted felon from other charges that do not require proof of a prior conviction." Hackney, 28 Va. App. at 295, 504 S.E.2d at 389. This is a sensible rule, as evidence of *prior* convictions is both highly prejudicial and entirely unrelated to the joined offenses. Evidence in criminal cases is usually prejudicial, otherwise it would not normally be relevant. To render otherwise relevant evidence inadmissible, the probative value of

the evidence must be *substantially* outweighed by its prejudicial effect. Va. R. Evid. 2:403. Here, in the context of the charges and the evidence presented, the effect of the pornographic videos is no more prejudicial than an analogous situation where a defendant is on trial for possession of both cocaine and heroin and the evidence is that the cocaine was in his right pocket and the heroin in his left. Moreover, despite Stickle's protestations to the contrary, the evidence of the videos in which he is featured is directly related to the other charges and highly probative of both his knowledge that child pornography was on his computer and that he intended for child pornography to be distributed. "Evidence of other crimes or convictions may be admitted for the purpose of, among other things, . . . proving a relevant issue or element of the offense charged, such as motive, intent, common scheme or plan, knowledge or identity." Hackney, 28 Va. App. at 293, 504 S.E.2d at 388 (internal citations omitted). Thus, we find no error in the circuit court's conclusion that justice did not require severance of the charges involving the videos from the remaining charges.

C. Sufficiency of the Evidence

Stickle finally argues that the Commonwealth had no actual evidence that he knew the child pornography in the ARES folder was on the laptop and that the Commonwealth is "bootstrapping" knowledge of the three videos which Stickle created into knowledge of the twenty-two other pieces of pornography, despite the fact that they are located on different parts of the computer.

"When considering the sufficiency of the evidence to sustain a conviction, we examine the evidence in the light most favorable to the Commonwealth, the prevailing party at trial, granting it all reasonable inferences fairly deducible therefrom." Jordan v. Commonwealth, 286 Va. 153, 156, 747 S.E.2d 799, 800 (2013) (citing Dowden v. Commonwealth, 260 Va. 459, 461, 536 S.E.2d 437, 438 (2000)). "We will not set aside the trial court's judgment unless it is 'plainly wrong or without

evidence to support it.'" Kelley v. Commonwealth, 289 Va. 463, 468, 771 S.E.2d 672, 674 (2015) (citing Code § 8.01-680).

The evidence taken in the light most favorable to the Commonwealth did show that Stickle had roommates at various times who occasionally used his computer. It also showed that his fiancée Mallory had used his computer at least once. However, none of these roommates remained as such during the entire span of time videos were placed on Stickle's computer. Additionally, Little only began detecting child pornography present at Mallory's IP address after Stickle moved in with her. All images were within a password-protected user account which also contained the three videos of Stickle himself performing sexual acts with a child. An oft-quoted maxim of our jurisprudence is that "[t]he Commonwealth need only exclude reasonable hypotheses of innocence that flow from the evidence, not those that spring from the imagination of the defendant." Hamilton v. Commonwealth, 16 Va. App. 751, 755, 433 S.E.2d 27, 29 (1993). Stickle's contention is entirely unsupported speculation clearly rejected by the jury rather than reasonable inferences flowing from the evidence, and it was unnecessary for the Commonwealth to exclude them. The jury was entitled to reject Stickle's assertion that for many years an interstate cabal of roommates and fiancées used his computer without his knowledge to store child pornography, and we hold that the evidence was legally sufficient for the jury to instead conclude beyond a reasonable doubt that the child pornography was knowingly possessed and possessed with the intent to distribute by a man with such an interest in child pornography that he created his own videos.

III. Conclusion

Upon review of the record, we find no error in the trial court's decisions to admit the evidence and to join the charges. We also find that the evidence was sufficient to convict Stickle on all charges. The judgment of the trial court is therefore affirmed.

Affirmed.