2018 WI App 63

COURT OF APPEALS OF WISCONSIN
PUBLISHED OPINION

Case No.: 2017AP185-CR

Complete Title of Case:

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

RONALD LEE BARIC,

DEFENDANT-APPELLANT.

Opinion Filed:	September 18, 2018
Submitted on Briefs:	December 11, 2017
Oral Argument:	

JUDGES:	Stark, P.J., Hruz and Seidl, JJ.
Concurred:	
Dissented:	

Appellant ATTORNEYS:	On behalf of the defendant-appellant, the cause was submitted on the briefs of *John Miller Carroll* of *John Miller Carroll Law Office*, Appleton.
Respondent ATTORNEYS:	On behalf of the plaintiff-respondent, the cause was submitted on the brief of *Brad D. Schimel*, attorney general, and *Scott E. Rosenow*, assistant attorney general.

2018 WI App 63

COURT OF APPEALS
DECISION
DATED AND FILED

September 18, 2018

Sheila T. Reiff
Clerk of Court of Appeals

Appeal No. 2017AP185-CR **Cir. Ct. No. 2015CF606**

STATE OF WISCONSIN **IN COURT OF APPEALS**

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

RONALD LEE BARIC,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Outagamie County: JOHN A. DES JARDINS, Judge. *Affirmed*.

Before Stark, P.J., Hruz and Seidl, JJ.

¶1 SEIDL, J. Ronald Baric appeals a judgment entered following his no-contest pleas, convicting him of two counts of possession of child

pornography, contrary to WIS. STAT. § 948.12(1m) (2015-16).[1] Baric contends the circuit court erred by denying his motions to suppress evidence of child pornography seized from his computers and hard drives. Specifically, Baric contends the evidence should have been suppressed because: (1) the police conducted an illegal, warrantless search when they viewed files he offered for download on a peer-to-peer (P2P) file sharing network; and (2) he was coerced into consenting to a subsequent search of his computer devices. We conclude that Baric had no reasonable expectation of privacy in files he offered for download on a P2P file sharing network and that he voluntarily consented to the search of his computer devices. Thus, we affirm.

BACKGROUND

¶2 In October 2014, Shawano County Detective Gordon Kowaleski discovered evidence that a computer located in Wisconsin contained ten files of child pornography. Kowaleski located the evidence by using a software program called Child Protection System (CPS) to conduct an automated search of P2P file sharing networks for known files of child pornography.

¶3 P2P file sharing is a means by which computer users share digital files with other users around the world. The only requirements to access a P2P file sharing network are that a user have an internet connection and P2P software.[2] In this case, Baric used the P2P software program eMule to connect to the P2P file

[1] All references to the Wisconsin Statutes are to the 2015-16 version unless otherwise noted.

[2] For additional information on P2P networks, see *P2P definition*, TechTerms.com, https://techterms.com/definition/p2p (last visited Sept. 12, 2018).

sharing network eDonkey. In other words, Baric logged on to the eDonkey network by running eMule software.

¶4 In addition to having P2P software, a user must have an internet connection in order to connect to a P2P network. This requires the user to make his or her internet protocol (IP) address available, because without doing so, he or she cannot connect to other users on the network to share files. An IP address is a "unique address that identifies a device on the Internet."[3]

¶5 When a file is shared on a P2P network, it is assigned a unique digital signature, known as a hash value. A hash value assigned to a file remains constant, even if the file name is changed. When a P2P user selects a file to download, the P2P software searches the P2P network for all users that have shared a file with the corresponding hash value. The P2P software then connects to those users to download the file. Law enforcement has compiled a list of hash values assigned to files of known child pornography. By using this list, they are able to search a P2P network and identify users who are sharing files of child pornography.

¶6 The CPS software that Kowaleski employed in his October 2014 search conducted an automated search of files on P2P networks, including eDonkey, that users had made publicly available for download. One particular IP address that Kowaleski's search identified as sharing files with hash values matching known files of child pornography was located in Wisconsin.

[3] For additional information on IP addresses, see *IP Address Definition*, TechTerms.com, https://techterms.com/definition/ip_address (Last visited Sept. 12, 2018).

¶7 Accordingly, Kowaleski served a subpoena on Charter Communications, the internet service provider for the captured IP address, and found that the registered subscriber for that particular IP address was John Schultz, located in Hortonville. Kowaleski provided Schultz's address to the Wisconsin Department of Justice, and Special Agent Jed Roffers took over the investigation. Roffers determined that Schultz shared his residence with several individuals, including Baric, and that Baric was well-versed with computers. He also learned that Susan Schultz, John's wife and Baric's sister, ran an in-home daycare at the residence.

¶8 In February 2015, Roffers and Special Agent Chad Racine went to Schultz's home to interview its residents. They decided to first focus on Baric because of his familiarity with computers. They approached the house at approximately 8:00 p.m., both dressed in plain clothes. Susan let them into the home, and Roffers and Racine identified themselves as law enforcement officers. Roffers asked if he could speak with Baric, who was downstairs in his bedroom, so Susan asked Baric if he would come upstairs to speak with the agents. Once Baric came upstairs, Roffers and Racine began to question Baric about his computer use. Susan initially remained in the room and participated intermittently in the conversation.

¶9 Baric told the agents that he was twenty-seven years old and had a degree in computer science. He rated his knowledge of computers, on a scale of one-to-ten "with 10 being Bill Gates," as an eight. Roffers asked Baric if he knew what P2P file sharing was, and Baric told him he did. Baric then admitted to illegally downloading music. Roffers told Baric that he did not investigate illegal music downloads, and that his investigations focused on the exploitation of children on the internet. Roffers asked Baric if he would allow a forensic analyst

to look at his laptop. Baric initially said he would allow the inspection, if Roffers thought one had to be performed. Roffers responded that the decision to allow the inspection was "completely up to" Baric. Baric responded, "I would rather not, no."

¶10 Roffers then told Baric he thought there might be concerning files on the laptop, especially given that Susan ran a daycare in the house. Baric said that he had "an idea" what Roffers was talking about. At that point, Roffers asked if Baric wanted to continue their conversation in private. Baric said he did, and Roffers and Racine continued the interview with just Baric present. Roffers told Baric he was not under arrest and he was not in custody, but that Roffers wanted to talk to him. Roffers then explicitly told Baric he was investigating child pornography, and he asked Baric if there was a possibility he may have viewed any child pornography. Baric told Roffers he may have viewed some pornography with "teenagers ... like 16 and up." Baric went on to admit he may have seen pornography involving children as young as fourteen or fifteen.

¶11 Roffers again told Baric that he was especially concerned about his internet activity because there were often children present in the house with Baric. Baric said he only had viewed the child pornography out of curiosity, but he would never "act on it at all." He then said he had viewed "pre-teen" child pornography and it disturbed him. Roffers asked if Baric's computer may have those kinds of files on it, and Baric said that he did not think so because he usually deletes those files that disturb him. Roffers told Baric he thought that, at this point, Baric knew what the right thing to do was. Baric said he did, and it was "[c]ooperating as much as I can."

¶12 After Roffers agreed with Baric that it was in his best interest to be cooperative, Baric told him "I know it's wrong ... I'm just scared I guess." Racine said he understood, but Baric had to take responsibility for his mistakes. Baric again said he knew "it's wrong," and he "want[ed] to do what I can to cooperate." Roffers asked if Baric would take the agents down to see his bedroom, and Baric agreed to do so.

¶13 While Baric took Roffers downstairs to his bedroom, Racine retrieved a consent form, which Baric eventually read. The form indicated that Baric had the right to refuse to consent to any search and that if he did consent, anything found could be used against him in criminal proceedings. Baric asked if the agents would take his computer with them if he consented to the search. Roffers said they would not take anything with them unless they found something concerning during an initial, on-site preview. Baric signed the form, and the agents took two computers and three hard drives outside the house. A computer forensic analyst that had been waiting there conducted an on-site preview on the devices, and she discovered several videos and images of child pornography.

¶14 The State charged Baric with ten counts of possession of child pornography. Baric filed a motion to suppress, arguing that he did not voluntarily consent to the search of his computer devices. The circuit court held an evidentiary hearing, at which Roffers, Baric and Susan testified. The court denied Baric's motion in a written order, finding that the "gentle questioning" by Roffers and Racine did not exceed Baric's ability to resist and that there was "no coercion." Therefore, the court concluded Baric's consent was voluntary and constitutionally valid.

¶15 Baric then filed a second motion to suppress. Baric argued in this motion that Kowaleski performed an illegal search when he located and viewed the files that Baric made publicly available on the eDonkey P2P file sharing network. After a hearing, the circuit court denied the motion in an oral decision, concluding there is no reasonable expectation of privacy in files shared on the internet and, therefore, no search occurred within the meaning of the Fourth Amendment.

¶16 Pursuant to a plea agreement, Baric pled no-contest to two counts of possession of child pornography. The remaining counts were dismissed but read in for sentencing. The circuit court imposed concurrent sentences consisting of three years' initial confinement and four years' extended supervision on both counts. Baric now appeals, arguing that the circuit court erred by denying his suppression motions.

DISCUSSION

A. P2P file sharing

¶17 Baric first contends that his constitutional right to be free from unreasonable searches and seizures was violated when Kowaleski viewed the digital files Baric made available on the eDonkey P2P file sharing network. The Fourth Amendment to the United States Constitution protects against unreasonable

searches and seizures.[4] ***State v. Young***, 2006 WI 98, ¶18, 294 Wis. 2d 1, 717 N.W.2d 729. This protection, however, extends only to areas in which there is a reasonable expectation of privacy. ***State v. Guard***, 2012 WI App 8, ¶16, 338 Wis. 2d 385, 808 N.W.2d 718. Therefore, to challenge a search on Fourth Amendment grounds, a defendant must first show two things by a preponderance of the evidence: "(1) that he or she had an actual, subjective expectation of privacy in the area searched and item seized and (2) that society is willing to recognize the defendant's expectation of privacy as reasonable." ***State v. Tentoni***, 2015 WI App 77, ¶7, 365 Wis. 2d 211, 871 N.W.2d 285.

¶18 Here, we focus on the second prong of the test—that is, whether Baric had an objectively reasonable expectation of privacy in files that he shared on a P2P network.[5] The following non-exclusive factors are relevant to the objective reasonableness inquiry:

> (1) whether the defendant had a property interest in the premises; (2) whether he [or she] was legitimately (lawfully) on the premises; (3) whether he [or she] had complete dominion and control and the right to exclude others; (4) whether he [or she] took precautions customarily taken by those seeking privacy; (5) whether he [or she] put the property to some private use; and (6) whether the claim of privacy is consistent with historical notions of privacy.

[4] Baric bases his argument solely on the Fourth Amendment to the United States Constitution. However, in the interest of thoroughness, we note that Article I, Section 11 of the Wisconsin Constitution also protects the right to be secure against unreasonable searches and seizures. ***State v. Dearborn***, 2010 WI 84, ¶14, 327 Wis. 2d 252, 786 N.W.2d 97. Historically, Wisconsin courts have interpreted the "Wisconsin Constitution's protections in this area identically to the protections under the Fourth Amendment as defined by the United States Supreme Court." ***Id.***

[5] We do not address the first prong of the test—whether Baric had an actual, subjective expectation of privacy in the files he shared—because the second prong is dispositive. *See* ***Sweet v. Berge***, 113 Wis. 2d 61, 67, 334 N.W.2d 559 (Ct. App. 1983).

State v. Dumstrey, 2016 WI 3, ¶47, 366 Wis. 2d 64, 873 N.W.2d 502 (citation omitted). Although these factors guide our analysis, they are not controlling. ***Tentoni***, 365 Wis. 2d 211, ¶7. We consider the totality of the circumstances in determining whether an individual has a reasonable expectation of privacy. ***Id.***

¶19 We note that by analyzing the reasonableness of Baric's expectation of privacy under the traditional Fourth Amendment framework, we implicitly acknowledge that the expectation of privacy in digital files—a new and particular issue for Wisconsin courts—is governed by the same standards as the expectation of privacy in physical property. For the sake of clarity, we explicitly state just that: the reasonableness of an expectation of privacy in digital files shared on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context.

¶20 We review the circuit court's denial of Baric's motion to suppress under a two-step inquiry. *See* ***State v. Lonkoski***, 2013 WI 30, ¶21, 346 Wis. 2d 523, 828 N.W.2d 552. First, we uphold the court's findings of fact unless they are clearly erroneous. ***Id.*** Second, we independently apply constitutional principles to those facts. ***Id.*** The question of whether a Fourth Amendment search has occurred—which, as stated above, Baric bears the burden to show by a preponderance of the evidence—is a question of law that we review independently. *See* ***Guard***, 338 Wis. 2d 385, ¶14.

¶21 After considering the factors applicable to this case, we agree with the State that Baric did not have an objectively reasonable expectation of privacy in files he publicly shared on a P2P file sharing network. Baric had no property interest in the eDonkey file sharing network, and once he made the files publicly available for download, he did not have any dominion or control over the files. He

could not prevent anyone, including law enforcement, from accessing the P2P network and viewing the files that he offered to share.[6]

¶22 We note that courts in other jurisdictions have uniformly reached the conclusion that individuals have no objectively reasonable expectation of privacy in files shared on P2P networks. *See, e.g.*, ***United States v. Conner***, 521 F. App'x 493, 498 (6th Cir. 2013) (noting that federal circuit courts of appeal "uniformly hold that there is no reasonable expectation of privacy in files the government obtained using peer-to-peer sharing services."); ***State v. Roberts***, 2015 UT 24, ¶25, 345 P.3d 1226 (holding "there is no reasonable expectation of privacy in a file that an individual publicly shares on a P2P network"); ***State v. Combest***, 350 P.3d 222, 230 (Or. Ct. App. 2015) (holding officers' use of software to download files on a P2P network did not constitute a search because there was no protected privacy interest in the files).

¶23 In response, Baric argues that Kowaleski subjected him to an unreasonable search under ***Kyllo v. United States***, 533 U.S. 27 (2001). In ***Kyllo***, the Supreme Court held that the use of thermal imaging scanners to surveille a home was a search within the meaning of the Fourth Amendment. ***Id.*** at 40. The Court reasoned that because the thermal imagers were not publicly available and revealed "details of the home that would previously have been unknowable without physical intrusion," a constitutional search occurred. ***Id.*** Baric attempts to analogize the use of CPS software, which is not publicly available, to the

[6] In his reply brief, Baric argues that because a file shared on a P2P network is stored on a user's computer, not a server, and then shared directly to other P2P users, the file is somehow not held out to the public. This argument is illogical and admits that a P2P user indiscriminately allows all other P2P users direct access to shared files stored on the user's computer.

thermal imager in ***Kyllo*** because it is a "sense enhancing device." Even assuming, without deciding, that CPS software is a sense enhancing device not publicly available, we are not persuaded by Baric's analogy. Although ***Kyllo*** involved the use of non-publicly available technology, its holding still focused on the requirement that an individual have a privacy interest in the area searched in order for the Fourth Amendment to apply. ***Id.*** at 33. The intrusion in ***Kyllo*** involved the privacy of one's home, which is unlike here, where law enforcement was searching electronic files held out for view to the public.

¶24 To expand on this distinction, the CPS software did nothing more than conduct an automated search that any member of the public could have performed manually to find the files on Baric's computer. *See* ***United States v. Dodson***, 960 F. Supp. 2d 689, 692-93 (W.D. Tex. 2013) ("CPS essentially automates the searches any normal human user can run on eMule and then stores the relevant information in a special law enforcement database. The program cannot search for private files on a computer if that user has not elected to make his [or her] files public."). Thus, any member of the public could use eMule to search the eDonkey P2P network and view Baric's digital files, just as Kowaleski did. ***Kyllo*** does not control our conclusion here because Baric has not shown by a preponderance of the evidence that he had a reasonable expectation of privacy in files he publicly shared for download on a P2P file sharing network.

¶25 Baric also argues Kowaleski performed an illegal search by using software to "geolocate" Baric using his IP address. In addition to being undeveloped, this argument fails on the merits. As stated above, to access a P2P network, a user must make his or her IP address publicly available. Once publicly available, "geolocation services ... enable anyone to estimate the location of Internet users based on their IP addresses. Such services cost very little or are

even free." ***AF Holdings, LLC v. Does 1-1058***, 752 F.3d 990, 996 (D.C. Cir. 2014). Again, Baric has not shown by a preponderance of the evidence that he had a reasonable expectation of privacy in either his IP address, which he made publicly available in order to access the P2P network, or his geolocation.[7]

¶26 In sum, we hold that there is no reasonable expectation of privacy in digital files that are publicly shared on a P2P network. Accordingly, we conclude that the circuit court properly denied Baric's motion to suppress based on these grounds.

B. Consent to search

¶27 Baric also contends he did not give valid consent to the search of his computer devices because his consent was coerced. "The Fourth Amendment to the United States Constitution and Article I, Section 11 of the Wisconsin Constitution prohibit unreasonable searches and seizures."[8] ***State v. Artic***, 2010 WI 83, ¶28, 327 Wis. 2d 392, 786 N.W.2d 430. A warrantless search is per se unreasonable, unless one of several clearly delineated exceptions to the warrant requirement applies. ***Id.***, ¶29. One such exception exists for searches conducted

[7] Baric raises two additional arguments. First, that Kowaleski acted outside of his jurisdiction because he used "engineered software contained on the CPS server down in Florida [to reach] into many servers across the country." And second, that Kowaleski acted outside the scope of his deputization because Kowaleski was not working directly with an FBI agent during his search. However, Baric fails to cite any legal authority or develop any meaningful analysis in support of either argument. We will not consider these undeveloped arguments. *See* ***State v. Pettit***, 171 Wis. 2d 627, 646, 492 N.W.2d 633 (Ct. App. 1992) ("We may decline to review issues inadequately briefed.").

[8] Baric, although represented by counsel, fails to articulate whether this claim is based on a violation of either the state or federal constitution. However, again, in the interest of thoroughness, we recognize the relevant authority.

pursuant to a party's consent.[9] ***Id.*** To determine whether the consent exception is satisfied, we consider: (1) whether consent was, in fact, given; and (2) whether the consent was voluntary. ***Id.***, ¶30. Here, Baric does not dispute that he consented in fact to the search of his computers when he signed the consent form; he challenges only the voluntariness of his consent.

¶28 The State bears the burden of proving by clear and convincing evidence that Baric voluntarily consented to the search. *See* ***Id.***, ¶32. Voluntariness of consent is a question of constitutional fact. ***Id.***, ¶23. As such, we accept the circuit court's findings of fact unless they are clearly erroneous, but we independently apply the constitutional principles to those facts to determine whether Baric's consent was voluntary. *See* ***Id.***

¶29 When evaluating the voluntariness of a party's consent to a search, we consider "the totality of all the surrounding circumstances." ***Id.***, ¶32 (quoting ***Schneckloth v. Bustamonte***, 412 U.S. 218, 226 (1973)). To qualify as voluntary, a party's consent must be an essentially free and unconstrained choice that is not the product of duress or coercion, whether express or implied. ***Id.*** The following non-exclusive factors are relevant to the voluntariness inquiry:

> (1) whether the police used deception, trickery, or misrepresentation in their dialogue with the defendant to persuade him [or her] to consent; (2) whether the police threatened or physically intimidated the defendant or

[9] Although Baric argues that Roffers and Racine "failed to properly attain freely given consent," and he seeks to suppress the evidence seized from his computer devices, his argument relies almost exclusively on ***State v. Hoppe***, 2003 WI 43, 261 Wis. 2d 294, 661 N.W.2d 407. However, ***Hoppe*** concerns the suppression of involuntary statements, not the suppression of evidence seized pursuant to involuntary consent. ***Id.***, ¶1. We agree with the State that the controlling law regarding the voluntariness of consent to search is ***State v. Artic***, 2010 WI 83, 327 Wis. 2d 392, 786 N.W.2d 430.

> "punished" him [or her] by the deprivation of something like food or sleep; (3) whether the conditions attending the request to search were congenial, non-threatening, and cooperative, or the opposite; (4) how the defendant responded to the request to search; (5) what characteristics the defendant had as to age, intelligence, education, physical and emotional condition, and prior experience with the police; and (6) whether the police informed the defendant that he [or she] could refuse consent.

Id., ¶33. We determine that, on balance, all of these factors support the circuit court's determination that "Baric was not coerced" and that the State has shown by clear and convincing evidence that Baric's consent to the search of his computer devices was voluntary.[10]

¶30 Regarding the first factor, the agents did not engage in deception, trickery, or misrepresentation. The agents identified themselves when they arrived at Schultz's house and forthrightly told Baric that they were investigating internet activity. After briefly discussing Baric's illegal music downloads, the conversation shifted to child pornography, and Roffers asked if Baric would like to speak in private. Baric said that he did, and the interview continued with just Baric, Roffers, and Racine present. Once in private, Roffers told Baric that he was not in trouble, he was not under arrest, and he was not in custody. Roffers

[10] The appellate record contains a transcript of Baric's interview with agents Roffers and Racine that the circuit court cited in its written decision denying Baric's motion to suppress. The court did not make explicit findings on all the contents of this transcript, but it is implicit in the court's decision that it accepted the contents of the transcript as accurate. We therefore treat the transcript as historical fact. *See* ***Town of Avon v. Oliver***, 2002 WI App 97, ¶23, 253 Wis. 2d 647, 644 N.W.2d 260. And although the court did not explicitly address the ***Artic*** factors, presumably due to the failure of Baric's counsel to raise them, we assume the court implicitly made the findings necessary to support its conclusion. *See* ***Town of Avon***, 253 Wis. 2d 647, ¶23. Furthermore, we note in our analysis where the court did make explicit findings that inform our consideration of particular ***Artic*** factors.

candidly told Baric, however, that "[Racine] and I, our primary concern [is] child pornography."

¶31 Baric argues Roffers made "patent misrepresentations" when he told Baric that he was not in any trouble and that Baric "might even know more about [computers]" than Roffers did. We agree with the State that these statements were, in fact, honest. First, when the agents told Baric he was "not in trouble," Baric was only one among a number of residents in a house where the agents believed someone possessed child pornography. Although Baric was a suspect at the time Roffers made the statement, Roffers had no evidence proving Baric was the person at the house who actually possessed the child pornography. Thus, it was a true statement that Baric was not yet in trouble. And even if there were evidence incriminating Baric, there was no attempt to trick Baric, as the agents explicitly told him they were investigating the downloading of child pornography.

¶32 Second, Roffers' statement that Baric might know more about computers than Roffers came after Baric rated his knowledge of computers as an eight on a one-to-ten scale. In light of this, Roffers' statement was not a misrepresentation. It was nothing more than an admission that Baric might have known more about computers than Roffers.

¶33 Regarding the second ***Artic*** factor, the circuit court found the agents did not threaten or physically intimidate Baric. That finding is not clearly erroneous. Roffers did tell Baric they could have procured a search warrant and "bust[ed] down the door and all that." But Roffers immediately told Baric that they chose not to do that, because there was no indication that Baric had a criminal history. Roffers testified that he believed he had grounds to secure a search warrant, and the circuit court found his testimony credible. A genuine statement

by law enforcement that they could procure a search warrant does not constitute a threat that renders consent involuntary. ***Artic***, 327 Wis. 2d 392, ¶¶41-42.

¶34 As to the third ***Artic*** factor, based on the circuit court's finding that the agents engaged in "gentle questioning," which is not clearly erroneous, the conditions of Baric's interview were congenial and cooperative. The agents told Baric that he was not under arrest and was not in custody, and they questioned him in what the circuit court found to be a "conversational tone." Further, Baric told the agents that he wanted to cooperate and he led the agents to his bedroom, where he told them they would find evidence of child pornography on his computer. Baric's actions support a determination of voluntary consent. *See* ***State v. Nehls***, 111 Wis. 2d 594, 599, 331 N.W.2d 603 (Ct. App. 1983) (holding a person's cooperation in leading law enforcement to evidence supports a determination of voluntary consent).

¶35 Under the fourth ***Artic*** factor, the record reflects that Baric's response to Roffers' initial request to search his computer was, "[i]f you wanted to, yeah." It was only after Roffers informed Baric that whether a search of his computer would occur at that time was completely up to him that Baric said he would "rather not" allow a search of his computer. The circuit court found that this constituted a refusal. However, the court also found that Baric's later consent was still "freely and voluntarily given." The record supports this conclusion.

¶36 Roffers did not indicate that Baric had to allow the search after the initial refusal, but he did tell Baric he was especially concerned about the possibility of someone downloading child pornography in a residence with an in-home daycare. Baric said that he understood and that he wanted to cooperate as much as he could. Baric's equivocation, when considered in context of his initial

consent and subsequent reaffirmation that he wanted to cooperate as much as he could, does not support a determination that his consent was involuntary.

¶37 The fifth ***Artic*** factor requires consideration of Baric's personal characteristics. He was twenty-seven years old at the time with a full-time job and a college degree in computer science. He rated his knowledge of computers at an eight on a one-to-ten scale. Those characteristics strongly suggest Baric knew exactly what a search of his computer would entail and what evidence law enforcement could recover. These personal characteristics support a determination that Baric's consent was voluntary.

¶38 Turning to the final ***Artic*** factor, Baric was told repeatedly that he had the right to refuse to consent to the search. Roffers told Baric that the decision to allow a search of his computers was "completely up to" him, and Racine told him that consenting to a search "isn't something that you have to do." Although there is no dispute that Baric was not read a ***Miranda***[11] warning, the lack of such a warning is not a dispositive factor in determining the voluntariness of his consent. *See* ***State v. Lemoine***, 2013 WI 5, ¶33, 345 Wis. 2d 171, 827 N.W.2d 589. Here, because Baric was repeatedly told he had the right to refuse his consent to a search and nevertheless chose to consent, there is no indication he would have refused to consent to the search if he had been read his ***Miranda*** rights.

¶39 For all these reasons, the totality of the circumstances demonstrates that Baric voluntarily consented to the search of his computer devices.

[11] ***Miranda v. Arizona***, 384 U.S. 436 (1966).

Accordingly, we conclude Baric's suppression motion on this ground was properly denied.

By the Court.—Judgment affirmed.