

IN THE
APPELLATE COURT OF ILLINOIS
SECOND DISTRICT

THE PEOPLE OF THE STATE)	Appeal from the Circuit Court
OF ILLINOIS,)	of Kane County.
)	
Plaintiff-Appellee,)	
)	
v.)	No. 04--CF--2441
)	
ROBERT S. PRINZING,)	Honorable
)	Timothy Q. Sheldon,
Defendant-Appellant.)	Judge, Presiding.

JUSTICE BOWMAN delivered the opinion of the court:

After a bench trial, defendant, Robert S. Prinzing, was convicted of possessing child pornography (720 ILCS 5/11--20.1(a)(6) (West 2004)) and sentenced to 30 months' probation. On appeal, he argues that the circuit court erred in denying his motion to suppress evidence, which maintained that the police illegally obtained his consent to search, through the use of trickery, deceit, or subterfuge. Defendant alternatively argues that, even if his consent was valid, the evidence should have been suppressed because the police exceeded the scope of his consent. We agree that the police exceeded the scope of the consent, and we reverse and remand.

I. BACKGROUND

On February 18, 2005, defendant was indicted for nine counts of possession of child pornography. The indictment alleged that on or about May 25, 2004, defendant knowingly possessed

pornographic computer images of children whom he knew or reasonably should have known to be under the age of 18.

On February 4, 2005, defendant moved to quash the search and to suppress evidence that was obtained. In his motion, he stated that on October 29, 2003, Detective Keith Smith of the Kane County sheriff's department received information from a federal agent, Ronald Wolfick, regarding Kane County residents who had possibly purchased child pornography over the Internet. On November 18, 2003, Detective Smith was informed that defendant was one of those residents. On February 4, 2004, Detective Smith spoke to defendant's credit card company and was informed that there had been a disputed charge for his account number and that the account was closed and a new card was issued. He then obtained defendant's new credit card number and computer screen name. On May 25, 2004, Detective Smith and Detective Grimes¹ went to defendant's residence under the guise of interviewing him about "possible fraudulent charges made on his credit card." Defendant agreed to discuss that matter and provided his credit card number to Detective Smith. Detective Smith knew that the number matched one reported to have been used to subscribe to a particular Web site, and he asked defendant for permission to search his computer in regard to the fraudulent credit card charges. Defendant consented, and the officers inserted a forensic preview program into the computer and began searching for photographic images, not fraudulent credit card charges. Detective Smith then obtained oral and written statements from defendant and took the computer, which belonged to defendant's wife.

Defendant's motion further alleged that on May 26, 2004, Detective Smith asked defendant to pick up his wife's computer from the sheriff's office and conducted another interview with

¹ Detective Grimes' first name is not contained in the record.

defendant, which was audiotaped. After the interview, Detective Smith turned over the computer to defendant. Defendant argued that his consent to the search was involuntary because of the officers' trickery, deceit, or subterfuge. He argued further that the officers illegally obtained oral and written statements from defendant and illegally seized defendant's computers, digital cameras, and compact discs. Defendant argued that, because the search of the computer violated defendant's fourth amendment rights, the physical evidence and the statements subsequently obtained should have been suppressed.

On March 3, 2005, the trial court held an evidentiary hearing on defendant's motion to suppress. Detective Smith testified as follows. He was employed with the Kane County sheriff's department and assigned to computer crimes and forensics. On October 29, 2003, he spoke with Ronald Wolfick, a special agent with Immigration and Customs Enforcement. Wolfick provided Detective Smith with information regarding online credit card purchases of child pornography and provided the credit card number used, which belonged to defendant. Detective Smith obtained a subpoena and contacted the bank that issued the credit card. The bank told Detective Smith that a fraudulent charge had been reported around the time that the card was used to purchase child pornography. The bank relayed that a new account number had been issued. On May 25, 2004, Detective Smith, along with Detective Grimes, went to defendant's residence at approximately 5 p.m. in an unmarked car. Detective Smith identified himself and stated that he was investigating fraud involving defendant's credit card. Detective Smith inquired "as to his card usage, the geographical area [in which] he might have used it, also if it was ever out of his control and through the course of the conversation trying to determine if he had lost control of that card where someone else could have acquired his credit card numbers." Defendant retrieved his credit card and gave it to Detective

Smith. Detective Smith recognized the number as the one that had been used to purchase child pornography. Defendant told Detective Smith that he owned the credit card and maintained exclusive control over the card. Defendant stated that he used the card in the local area, when he went on trips, and occasionally for Internet purchases. Detective Smith asked defendant whether there had been any fraud reported on his credit card. Defendant stated that there had been an incident of fraud, his money was refunded, and he was issued a replacement card.

Detective Smith told defendant that if he used the card on the Internet, there was opportunity for others to steal his information. Detective Smith asked defendant if he still possessed the computer that he used to make Internet purchases. If there was any evidence of his system being compromised by unsafe Internet Web sites or a virus, it would likely be on the computer used to make Internet purchases. Defendant denied noticing any suspicious activity on his credit card. Defendant worked for Comcast and was very knowledgeable about computers, impressing Detective Smith. Defendant denied having any suspicion that the security on his computer had been compromised. Detective Smith testified that a virus could infect a computer when a person received a spam e-mail or visited a particular Web site embedded with the virus. He had an investigatory tool that allowed him to check for such viruses.

Detective Smith asked defendant if he could search his computer by using a special program, with the intent of trying to determine how his credit card information might have been stolen. Defendant consented. Defendant was present in the room when Detective Smith began the program, but he left the room several times. According to Detective Smith, he initially used a noninvasive tool to perform a "preview," which prevents any changes from happening to the computer when the system is turned off and on. The "preview" allows detectives to view the hard drive but prevents

them from making any changes to any of its files. Normally, after the "preview" program, Detective Smith would use a program called "Image scan." The image scan looks for images related to Web pages to get a history of pages that the user has visited. The program brings up thumbnail images from Web pages. Depending upon what is found, he then would use a tool that would look for viruses or any key stroke loggers, which capture key strokes and send the information to a remote location. Detective Smith began the search of defendant's computer by using the image scan program. He was looking for thumbnails with the Visa logo, not for child pornography. Detective Smith testified that he did not inform defendant that he believed that his credit card information had been used to access child pornography Web sites, because "at this point [he] didn't feel that [defendant] still had been--was the offender. [Detective Smith] was curious as to how his information could have been compromised." He was concerned that defendant's credit card may have been compromised not once, but twice. Detective Smith explained that "when you visit a web site, if you go to make a purchase, you will see a Visa logo. That will be captured. Whatever the merchandise is being offered on that particular web page, it will have graphics that will show that." A Visa credit card number will not be captured. Detective Smith would have to click on the image to get to the vendor's Web site.

Detective Smith found several images that he suspected were child pornography. He found the images within 10 to 15 minutes after he began the scan. He denied that he was specifically looking for child pornography. Rather, he was looking for information related to defendant's credit card. He considered his investigation up to this point to be related to credit card fraud because there was evidence of only a few attempts to access the pornographic Web sites, whereas other investigations involved numerous attempts. He stopped the search and asked "for consent, asked

[defendant] to grant another interview regarding the images that [he] had seen." Defendant agreed to speak to him again. Detective Smith testified:

"I explained to him that based on what he had told me that he had physical control of his credit card all the time and he had no reported compromises of his Internet service, was he familiar--I had some concern over the images and was he familiar with two particular web sites which I named for him."

Defendant believed that one of the named sites was one that he had previously subscribed to. The disputed charge on his credit card involved one of the sites. Defendant stated that he was relieved that this was "out" so that he could get it behind him. He never asked to end the conversation, and Detective Smith asked him to provide a written statement summarizing his credit card usage. Defendant agreed and provided a statement.

Detective Smith then told defendant that based on what he saw, he "had no choice but to take [defendant's] computers." Defendant was concerned about how long the computers would be gone, because one of the computers was his wife's work-related laptop. Detective Smith asked for and received oral and written consent to take the computers. Defendant assisted Detective Smith in gathering all the computers and media storage devices that were to be taken into evidence. Defendant asked Detective Smith whether he was going to be arrested, and Detective Smith stated that he did not know what the results would be of their computer analysis. He told defendant that the matter was still under investigation but that he would give him notice and an opportunity to turn himself in if he were to be arrested. The detectives then left defendant's home.

The next day, May 26, 2004, Detective Smith called defendant and advised that the police were finished with his wife's computer and that Detective Smith could drop it off to him. Defendant

stated that he could pick it up on his way home. When defendant arrived around 5 p.m., Detective Smith asked if he would consent to another interview and defendant agreed. Defendant agreed to have the interview audiotaped.

On cross-examination, Detective Smith admitted that he was specifically assigned to review cases that involved Internet child pornography. He admitted that the information that he received from Wolfick involved child pornography purchased on the Internet and was obtained through a federal investigation known as Operation Falcon. He admitted that Wolfick never mentioned credit card fraud. He admitted that, when he testified before the grand jury to obtain subpoenas for defendant's credit card records, he was investigating the possibility that defendant purchased child pornography. He admitted that he spoke with defendant's credit card company and was told that there was a disputed charge of \$565 on the card but that that account had been closed in June 2003. The bank told him that a new card had been issued, and he received both credit card numbers from Wolfick. The dates of the child pornography purchases were between May and June of either 2002 or 2003; Detective Smith could not recall the year in question.

Detective Smith admitted that he was investigating defendant between February 20, 2004, and May 25, 2004, for possession of child pornography and had obtained on that ground grand jury subpoenas for defendant's Internet service, credit card, and e-mail address. Although he had no information that suggested that someone other than defendant used his card to visit child pornography sites, Detective Smith maintained that he was not sure that defendant was the actual person visiting the sites. He admitted that he had no information that defendant's credit card had actually been used fraudulently. He never mentioned the words "child pornography" when he visited defendant's home, and he did not inform defendant that his card may have been used to purchase

child pornography. Detective Smith claimed that he did not provide defendant with this information because he had no suspicion that defendant visited the child pornography sites. Detective Smith admitted that he continued to ask him questions about his computer after defendant told him that the disputed charge had been resolved and that he had no concerns about credit card fraud.

Kathleen Ann Donovan, defendant's wife, testified as follows. She confirmed that Detective Smith and Detective Grimes arrived at her front door claiming that they were investigating potential fraud. The detectives asked about any fraudulent activity on their credit cards. She recalled having a dispute regarding some charges to their account but neither she nor her husband filed any police reports connected with that dispute. The detectives did not ask about any particular Web sites connected with any online purchases until after they inspected the computer. The detectives asked to look at the computer so that they could find evidence of any fraudulent credit card transactions. Defendant consented and later the detectives stated that they found child pornography images on the computer. They then began collecting all the computers in the home, three of which belonged to Donovan. She did not believe that she could stop the detectives from confiscating her computers. Detective Smith then asked defendant to make a written statement about the definition of pornography and had him sign a consent form that listed the computers that were being removed from the home.

On May 26, 2004, Detective Smith was supposed to meet Donovan at the train station in Geneva to return her computer to her. When she arrived at the station, he was not there. Defendant called her to inform her that the detective could not meet her there. Defendant stated that he would go pick up the computer from the police station.

Defendant testified next. Around 5 p.m. on May 25, 2004, two detectives arrived at defendant's home. They told him that they were investigating a fraud case, which he thought was unusual considering that he did not have any complaints regarding any type of fraud. The detectives questioned him for approximately 10 or 15 minutes regarding his credit cards and credit card numbers. They asked if he had a particular credit card but did not inform him how they had acquired his credit card information. He produced all of the credit cards in his wallet. He told Detective Smith that he had a disputed charge at one time but that it had been resolved and he had been issued a new card. He thought that perhaps the credit card number that the detectives had was his old card number. His disputed charge took place sometime in June 2003. He had another disputed charge in August 2003, but a new card was not issued then. The detectives asked about his card usage and whether he was the sole user. They then asked to view his computer to check for viruses that could have stolen his credit card information. Defendant stated that "Detective Smith asked to view [the] computer to look for viruses, you know, signs that [a] hacker had been in [defendant's] computer, Trojan horses, worms, anything that might possibly capture key strokes that [he] was typing in to get [his] credit card information." He initially told the detectives that he did not feel it was necessary, because he had several firewalls in place and felt secure in his computer usage. Detective Smith insisted that it would be better for him to check defendant's computer because his programs were better than anything that is available commercially. After the third request, defendant agreed to allow Detective Smith to check his computer.

Detective Smith then produced a USB port cable and a couple of disks that he retrieved from his briefcase. He inserted a disk into defendant's computer, rebooted it, and then began looking at images that were on the computer. Defendant stated that it appeared that the program was creating

files of pictures, because Detective Smith went to "a directory and [was] opening up different files, and every time he opened one up, it was populating with pictures from [the] computer." Defendant never saw any images with credit card logos; he saw only images that he had downloaded from the Internet or from his digital camera. Defendant was employed by Comcast, and he regularly checked systems for viruses. The programs he used to check for viruses never brought up images but only executable files. Viruses are not embedded in images but are executable programs. He thought it was odd that Detective Smith was looking only at pictures but defendant did not say anything. After about 15 to 20 minutes, Detective Smith stated that he was done looking at the computer and that he found an image that he felt was child pornography. Detective Smith then asked defendant about two Web sites and defendant admitted that he had visited them. Detective Smith then told defendant that he had to confiscate all the computers in the house and search all media that might contain pictures or other files. Detective Smith did not ask for permission to search the home for additional computers and media storage devices, such as defendant's digital camera. Defendant turned over these items because he did not feel that he had a choice.

On May 25, 2004, Detective Smith was scheduled to meet Donovan at the train station at 2 p.m. to return her work laptop computer to her. However, he called defendant at 1:30 p.m. and stated that he could not make it and could not stop by their home for several days. Instead, defendant offered to pick the computer up after work. Detective Smith agreed and, when defendant arrived at the police station around 5:15 p.m., Detective Smith asked if he would agree to be interviewed. Defendant agreed and provided a taped statement.

On May 19, 2005, the trial court denied defendant's motion to suppress. The trial court determined that Detective Smith was "steadfast" in his position that he went to defendant's residence

to investigate credit card fraud and that defendant consented to the search of his computer. After discovering the child pornography, Detective Smith stopped the search and obtained defendant's voluntary written statement and consent to seize the computers in the home. The next day, defendant agreed to go to the police station and agreed to be interviewed on tape. The trial court did not find that Detective Smith engaged in trickery, deceit, or subterfuge.

On July 14, 2005, defendant filed a motion to reconsider the denial of his motion to suppress. He argued that the trial court failed to consider all the testimony and failed to consider that Detective Smith's testimony was impeached by his grand jury testimony, and thus, the trial court erred in finding that defendant's consent to the computer search was valid. On February 24, 2006, the trial court denied defendant's motion for reconsideration. The trial court found that Detective Smith was not impeached because during his grand jury testimony he was only asked whether the tip he received was related to a child pornography investigation. He did not change this testimony at the motion to suppress hearing but was steadfast in his stance that his investigation began as one of potential credit card fraud. It further found that defendant did not do anything to attempt to stop the search and had voluntarily turned over various compact disks that contained images. The court did not ignore defendant's testimony or his wife's testimony but, rather, found that the testimony did not support defendant's position that Detective Smith used trickery to obtain his consent for the search and seizure of his computers or to obtain his written and taped statements.

On August 31, 2006, defendant filed a motion for reconsideration based on newly disclosed evidence. Defendant argued that he did not have the transcripts from the grand jury subpoena hearing when he filed his motion to suppress and earlier motion for reconsideration. According to defendant, the grand jury testimony directly impeached Detective Smith's testimony at the hearing

on defendant's motion to suppress. The sole witness at the grand jury hearing was Detective Smith, who testified that the subpoenas being sought were for the limited purpose of investigating child pornography cases. Detective Smith further testified that he was investigating five individuals implicated in a federal investigation and was "trying to determine if these people, in fact, had knowledge of that credit card and their Internet service provider accounts having been used." He was seeking information from the credit card companies to determine the accuracy of the information received about the suspected purchases. He answered "yes" when asked if the credit card information was being obtained solely for the purpose of investigating child pornography cases against the individuals.

The trial court denied this motion on October 18, 2006. In its ruling, the trial court stated that it believed that Detective Smith's investigation of defendant initially related to child pornography, morphed into a credit card fraud investigation when he discovered that there was a disputed charge on defendant's card, and then, after he discovered child pornography on defendant's computer, morphed back to a child pornography investigation.

The State nol-prossed counts three and eight, and the matter proceeded to a bench trial on the remaining seven counts. The trial court found defendant not guilty on count one and guilty on the remaining six counts. Defendant was sentenced to 30 months' probation on July 13, 2007, and this timely appeal followed.

II. ANALYSIS

When reviewing a trial court's ruling on a motion to suppress evidence, we apply a two-part standard of review adopted by the Supreme Court in *Ornelas v. United States*, 517 U.S. 690, 699, 134 L. Ed. 2d 911, 920, 116 S. Ct. 1657, 1663 (1996). *People v. Harris*, 228 Ill. 2d 222, 230 (2008).

Under this standard, we reject the trial court's findings of historical fact only if they are against the manifest weight of the evidence, and we review de novo the trial court's ultimate legal ruling as to whether suppression was warranted. *Harris*, 228 Ill. 2d at 230. In this case, the trial court believed Detective Smith when he claimed he was investigating credit card fraud and not child pornography when he sought defendant's consent to search his computer. We review this factual finding under the manifest weight of the evidence standard. We will review de novo the ultimate legal conclusion by applying fourth amendment rules to the facts.

It is well settled under the fourth and fourteenth amendments that warrantless searches are unreasonable subject only to a few established exceptions. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219, 36 L. Ed. 2d 854, 858, 93 S. Ct. 2041, 2043 (1973). One established exception to the warrant requirement is a search that is conducted with voluntary consent. *Schneckloth*, 412 U.S. at 219, 36 L. Ed. 2d at 858, 93 S. Ct. at 2043-44. It is the State's burden to show by a preponderance of the evidence that the consent was voluntary. *People v. Alvarado*, 268 Ill. App. 3d 459, 464 (1994). Whether consent was voluntary is a question of fact to be determined from the totality of the circumstances. *Schneckloth*, 412 U.S. at 227, 36 L. Ed. 2d at 863, 93 S. Ct. at 2048. The two competing concerns that must be accommodated in determining the meaning of a voluntary consent are: (1) the legitimate need for such searches and (2) the equally important requirement of assuring the absence of coercion. *Schneckloth*, 412 U.S. at 227, 36 L. Ed. 2d at 863, 93 S. Ct. at 2048. Whether consent was voluntary is a question of fact for the trial court, and its decision will not be disturbed unless it is against the manifest weight of the evidence. *People v. Smith*, 214 Ill. 2d 338, 350 (2005).

Courts may consider many factors when evaluating the totality of the circumstances. Knowledge of the right to refuse consent is one factor to be considered, but the State does not need to establish such knowledge to prove an effective consent. *Schneckloth*, 412 U.S. at 227, 36 L. Ed. 2d at 863, 93 S. Ct. at 2048. Factors surrounding coercion or duress are also considered. Consent is not voluntary where it is the result of coercion, intimidation, or deception. *People v. Graf*, 265 Ill. App. 3d 746, 750 (1994). An initial refusal to a police request to search is a factor that could demonstrate involuntariness. *Graf*, 265 Ill. App. 3d at 752. Further, consent obtained by means of deception may also be invalid. *People v. Daugherty*, 161 Ill. App. 3d 394, 399 (1987). While some forms of deception may not invalidate the consent, we must review the voluntariness of the consent in light of traditional notions of fairness and society's needs for effective police investigations. *Daugherty*, 161 Ill. App. 3d at 399. Here, defendant first alleges that his consent to the computer search was invalid because Detective Smith deceptively claimed that he was looking for evidence of computer viruses that could have led to credit card fraud when in fact he was looking for images of child pornography.

This leaves us to first determine whether the trial court's factual determination that Detective Smith did not engage in trickery, deceit, or subterfuge when he asked to search defendant's computer for fraudulent credit card activity is against the manifest weight of the evidence. Defendant likens his case to *Daugherty*. In *Daugherty*, police officers went to the defendant's home, identified themselves, and said that they wanted to discuss the theft that she reported a few days earlier. *Daugherty*, 161 Ill. App. 3d at 396-97. The theft case had already been solved, and, in the process of solving it, the police received information that marijuana was in the defendant's home. *Daugherty*, 161 Ill. App. 3d at 396. The defendant agreed to speak to the officers and let them inside her home.

Daugherty, 161 Ill. App. 3d at 396. The officers then asked to see where the theft had occurred, and the defendant showed them to the master bedroom; they then proceeded to the kitchen, where the officers saw marijuana on the counter. Daugherty, 161 Ill. App. 3d at 396-97. The trial court ruled that the real reason that the officers went to the defendant's home was to look for marijuana and that the theft investigation was just a ruse. This court agreed and also agreed that the officers' misrepresentation was so unfair that it rendered the defendant's consent invalid. Daugherty, 161 Ill. App. 3d at 400. We stated:

"Where, as here, the law enforcement officer without a warrant uses his official position of authority and falsely claims that he has legitimate police business to conduct in order to gain consent to enter the premises when, in fact, his real reason is to search inside for evidence of a crime, we find that this deception under the circumstances is so unfair as to be coercive and renders the consent invalid. *** This police conduct offends the fourth amendment and is fundamentally unfair when compared with the need for effective police investigation." Daugherty, 161 Ill. App. 3d at 400.

While Daugherty appears to be the only Illinois case invalidating consent on the ground that it was obtained through trickery, defendant also likens his case to those that invalidated consent on the ground that the police had misrepresented the defendants' rights. See *Bumper v. North Carolina*, 391 U.S. 543, 549-550, 20 L. Ed. 2d 797, 802-03, 88 S. Ct. 1788, 1791-92 (1968) (holding consent invalid when given under coercive circumstances in which police misrepresented that they had a warrant to search the home); *People v. Casazza*, 144 Ill. 2d 414, 418, 424 (1991) (finding consent invalid where the police officers misrepresented that, if the defendant would not consent to a search of his yacht, they could seize the yacht while they obtained a search warrant); *People v. Bailey*, 273

Ill. App. 3d 431, 437 (1995) (holding that consent was invalid where the defendant initially refused request for search and officers made unsupportable legal threat to detain the defendant's bag); *People v. Cardenas*, 237 Ill. App. 3d 584, 588-89 (1992) (finding consent to search vehicle invalid where the defendant initially refused request by stating " 'no, is that legal" and officers gave misleading information that they perform such searches regularly (emphasis omitted)); *People v. Purchase*, 214 Ill. App. 3d 152, 155 (1991) (finding consent to search home invalid where police officers made false threats to the defendant's wife that they would take her to jail and she would lose custody of her baby).

We find this case distinguishable from *Daugherty* and the other cases cited by defendant. It was undisputed that Detective Smith was informed by defendant's credit card company that there was a disputed charge that had been resolved by crediting back the charge and a new card number having been issued. It was also undisputed that the disputed charge in June 2003 was around the time that the child pornography Web site charges had been incurred. While Detective Smith did not mention the potential for child pornography purchases, he was not required to provide defendant with every piece of information that he possessed while investigating the matter. In *Daugherty*, the theft case had been resolved and the police employed purely deceptive tactics to obtain consent whereas, in this case, the police had not resolved whether the disputed credit card charge was related to the child pornography Web site charges. The remaining cases cited by defendant involved the police affirmatively misrepresenting the defendants' rights whereas here, the police made no such misrepresentations. Therefore, it was not against the manifest weight of the evidence to find that when Detective Smith asked for consent to search defendant's computer for viruses that may have compromised his credit card information, Detective Smith did not engage in trickery, deceit or

subterfuge, but, rather, he had a twofold purpose in his visit. Even if Detective Smith did use trickery, that would not necessarily render defendant's consent involuntary, as trickery is just one factor the court may consider in determining the validity of consent. See People v. Minnitti, 373 Ill. App. 3d 55, 69 (2007) (discussing effect of police trickery on voluntariness of confession).

Having determined that defendant's consent was voluntary, we now examine whether the police exceeded the scope of the consent. When determining whether a search is reasonable under the fourth amendment, we must determine first whether the officer's action was justified at its inception and second whether it was reasonably related in scope to the circumstances that justified the intrusion in the first place. People v. Lampitok, 207 Ill. 2d 231, 241 (2003). In evaluating the scope of a defendant's consent, the court considers what a reasonable person would have understood by the exchange between the officer and the defendant. People v. James, 163 Ill. 2d 302, 314 (1994). "[T]he parameters of a search are usually defined by the purpose of the search." James, 163 Ill. 2d at 314.

In this case, principles of law and technology collide. The court in People v. Berry, 314 Ill. App. 3d 1, 11-12 (2000), addressed the scope of consent with respect to electronic devices, specifically a cellular phone. Relying on various federal cases, the Berry court stated that the lack of knowledge of what the officer is searching for does not change the effect of a "general" consent. Berry, 314 Ill. App. 3d at 12. If a consent to search is entirely open-ended, a reasonable person would have no cause to believe that the search will be limited in some way, and the consent would include consent to search the memory of electronic devices. Berry, 314 Ill. App. 3d at 12. The Berry court then considered the totality of the circumstances, which involved a detective asking to look at the defendant's cell phone and the defendant responding "'go right ahead.'" Berry, 314 Ill. App. 3d

at 12. The officer, after receiving the defendant's response, opened the phone and retrieved the phone number of the phone by pressing a button. Berry, 314 Ill. App. 3d at 13. The defendant knew when the detective asked to search the phone that he was investigating a murder and that he was trying to determine whether the defendant owned the phone, and the defendant placed no explicit limitations on the scope of the search, either when he gave his general consent or while the officer examined the phone. Berry, 314 Ill. App. 3d at 14. Therefore, the court determined that, based on the totality of the circumstances, the detective did not exceed the scope of the defendant's general consent to search his phone when the detective activated the phone and retrieved the phone number. Berry, 314 Ill. App. 3d at 14.

Federal courts have also considered the scope of electronic device searches. In United States v. Lemmons, 282 F.3d 920, 925 (7th Cir. 2002), the court determined based on the totality of the circumstances that a police search did not exceed the defendant's general consent to search his computer. The police originally obtained consent to search for video recordings of the defendant's neighbor's bedroom. Once inside, the defendant showed police a sexually explicit photograph of his 17-year-old daughter. The police then asked whether there was anything on the defendant's computer that they should be aware of, and the defendant turned the computer on and invited the officers to look. Lemmons, 282 F.3d at 926. The officers then opened images saved on the computer that were pornographic images of children. Lemmons, 282 F.3d at 926. The court stated that the officers' search of the computer may have been illegal if the defendant had stuck to his original consent to search for a camera or recording device, or if he had limited his consent to search his computer to images of his neighbor, depending on the defendant's labeling system or other variables. Lemmons,

282 F.3d at 926. Because the defendant did not limit the consent to search his computer, the police did not exceed the scope by searching random images. Lemmons, 282 F.3d at 926.

In United States v. Brooks, 427 F.3d 1246, 1249 (10th Cir. 2005), the police requested to search the defendant's computer for child pornography by means of a "pre-search" disk. The police told the defendant that the pre-search disk would bring up all the images on the computer in a thumbnail format so that they could check for images of child pornography. Brooks, 427 F.3d at 1248-49. Defendant asked if it would search text files and he was told that it would not. For some reason, the disk was not operating on the defendant's computer, so the officers performed a manual search of images. Brooks, 427 F.3d at 1248. The defendant complained that the police exceeded the scope of his consent because they did not use the pre-search disk as he was told. The court disagreed, finding that the method in which the search was performed was irrelevant because the defendant knew that images would be searched and the officers searched only images and nothing more. Brooks, 427 F.3d at 1250.

We find this case distinguishable from Berry, Lemmons, and Brooks because those cases dealt with general consents to search. Here, Detective Smith, by his own words, limited the scope of the intended computer search. Detective Smith specifically requested to search defendant's computer for viruses or key-logging programs to find out if defendant's credit card number had been stolen. The exchange between Detective Smith and defendant involved only an investigation of credit card fraud and the potential that someone had stolen defendant's credit card number by way of a computer virus. By Detective Smith's own description of the scanning programs that he normally used, the image scan disk searched images and Web site pages on the computer. According to Detective Smith's testimony, if an image came up with a Visa logo, Detective Smith could click on

it and he would be brought to the Web page of the vendor. He did not testify that the vendor Web page would indicate whether defendant's credit card number was compromised. In fact, according to defendant, who worked for Comcast, no image would lead Detective Smith to discover a virus that could steal defendant's credit card number, as viruses and key-logging programs are executable files and not embedded in any image. Defendant consented to a search only for viruses, not images. Thus, we find that Detective Smith's search exceeded the scope of defendant's consent.

Our analysis is similar to the analysis in United States v. Richardson, 583 F. Supp. 2d 694, 716 (W.D. Pa. 2008). In Richardson, the police obtained consent to search the defendant's computer on the ground that they suspected "illegal" credit card activity over the Internet, insinuating that the defendant was a victim of credit card fraud. Richardson, 583 F. Supp. 2d at 713. The police then used a forensic image scanning disk to search the computer's hard drive for images, which the court determined exceeded the scope of the defendant's original consent to search for evidence of credit card fraud on the Internet. Richardson, 581 F. Supp. 2d at 716. The court noted that the officers chose to indicate to the defendant that they wanted to search for illegal credit card activity; they chose to impart to the defendant that he was a victim and not a suspect, and, thus, they chose to limit the scope of the search. Richardson, 581 F. Supp. 2d at 719. Likewise, Detective Smith made the same choices and must accept his self-imposed limitations on the search.

The State mentions that defendant did not object to the search when he saw Detective Smith bringing up images and that his failure to do so expanded the scope of the consent. The State failed to cite to any authority on this issue. Failure to cite to any authority results in forfeiture of the argument. 210 Ill. 2d R. 341(h); People v. Emerson, 189 Ill. 2d 436, 478 (2000). Regardless, we reject the State's argument on this point. Defendants have the right to place explicit limitations on

the scope of their consent and have the right to withdraw consent once it is given. People v. Baltazar, 295 Ill. App. 3d 146, 151 (1998). However, police officers remain constrained by the bounds of reasonableness in conducting their searches. Baltazar, 295 Ill. App. 3d at 151. Defendant's failure to object once Detective Smith began his search did not serve to transform his original limited consent to search for evidence of credit card fraud into a general consent to search all types of files and images on his computer. See Baltazar, 295 Ill. App. 3d at 151-52 (finding the defendant's failure to object to the police's exceeding of scope of original consent did not transform limited consent to general consent). If Detective Smith wanted a general consent from defendant, he should have refrained from including limitations in his request.

Having determined that Detective Smith exceeded the scope of defendant's consent, we review de novo the trial court's ultimate legal conclusion as to whether it should have granted defendant's motion to suppress, and we accordingly conclude that suppression was warranted. Further, the computer images were obtained through an illegal search, and defendant's ensuing statements were acquired within 24 hours of the search. The police did not present any new evidence to defendant in order to obtain his statements. As such, the evidence seized from defendant's home and his oral and written statements must be suppressed as there was no intervening event that broke the connection between the illegal search and the collection of evidence from the computers and his statements. See People v. Foskey, 136 Ill. 2d 66, 87 (1990) (finding that evidence obtained through illegal search and seizure must be suppressed unless there were intervening circumstances or events that were sufficient to purge the taint of the illegality).

III. CONCLUSION

Based on the foregoing reasons, we reverse the judgment of the circuit court of Kane County and remand for further proceedings consistent with this opinion.

Reversed and remanded.

SCHOSTOK, J., concurs.

JUSTICE O'MALLEY, dissenting:

Under the facts of this case, I would hold that any police deception had no bearing on the validity of defendant's consent, and I would hold that the search actually conducted fell within the scope of defendant's consent. I would therefore affirm defendant's conviction.

I begin by discussing the effect of the alleged police deception on the validity of defendant's consent. Illinois law provides unclear guidance on the point. The law as recited by the majority says at once that "[c]onsent is not voluntary where it is the result of official coercion, intimidation, or deception" (Graf, 265 Ill. App. 3d at 750), that consent obtained by deception may be invalid (Daugherty, 161 Ill. App. 3d at 399), that deception is a factor to be considered in assessing the voluntariness of a confession (Minniti, 373 Ill. App. 3d at 69), and that police tactics are unconstitutional where they are "purely deceptive" (as opposed to partially deceptive). See slip op. at 14, 16-17. These cases (and the majority) offer little to explain their conflicting views of the effect of police deception on consent. I therefore offer my own analysis of the issue.

Most authorities that would hold a consent procured by police deception to be invalid, including the Illinois cases cited by the majority, rely on the fourth and fourteenth amendment requirement that a consent be voluntary in order to be effective. Before the Supreme Court's 1973 decision in Schneekloth, which articulated the standards to be applied in determining the voluntariness of a consent to search, courts employed more elusive, and more subjective, measures of voluntariness. For example, in Alexander v. United States, 390 F.2d 101 (5th Cir. 1968), the Fifth Circuit rejected the argument that the defendant, who had been detained by postal inspectors, voluntarily consented to a search of his wallet, in part because the arrest may have coerced the

consent and in part because the postal inspectors told the defendant that they were looking for stolen jewels when they were actually looking for stolen (and marked) cash. On the latter point, the court opined that "[i]ntimidation and deceit are not the norms of voluntarism" and that, "[i]n order for the response to be free, the stimulus must be devoid of mendacity." Alexander, 390 F.2d at 110. The court went on to analogize the defendant's consent to a "fraudulently induced contract," and it stated that condoning police deception of the type at issue would "'obliterate one of the most fundamental distinctions between our form of government, where officers are under the law, and the police-state where they are the law.'" Alexander, 390 F.2d at 110, quoting United States v. Como, 340 F.2d 891, 894-95 (2d Cir. 1965), quoting Johnson v. United States, 333 U.S. 10, 17, 92 L. Ed. 436, 442, 68 S. Ct. 367, 370-71 (1948). The court thus concluded that "'civilized standards of fundamental fairness'" required that the consent be deemed involuntary. Alexander, 390 F.2d at 110, quoting Como, 340 F.2d at 894-95.

The Fifth Circuit's holding stood as a stern repudiation of consent induced by police deception of any kind. However, its reasoning was not unassailable, and its decision provided little practical guidance. On the former point, the analogy between consent to search on one hand and contract on the other has been rejected (see M. Friedman, Another Stab at Schneckloth: The Problem of Limited Consent Searches and Plain View Seizures, 89 J. Crim. L. & Criminology 313, 337 n.151 (1998) (hereinafter Friedman) (collecting cases)) and, in any event, is untenable due to the imbalance in bargaining power between police and suspect (Friedman, 89 J. Crim. L. & Criminology at 338) and also the failure of consideration. On the latter point, concepts of "fundamental fairness" prove too subjective to form the basis of a predictable standard for voluntariness. The Fifth Circuit found police deception antithetical to our notions of fairness, and other courts have since shared the opinion. For example, the Ninth Circuit has stated that individuals

should be able to rely on government agents' representations and thus held it " 'clearly improper for a government agent to gain access to records which would otherwise be unavailable to him by invoking the private individual's trust in his government, only to betray that trust.' " United States v. Bosse, 898 F.2d 113, 115 (9th Cir. 1990), quoting Securities & Exchange Comm'n v. ESM Government Securities, Inc., 645 F.2d 310, 316 (5th Cir. 1981). However, other courts, including the Supreme Court, have taken a more practical view. See Sherman v. United States, 356 U.S. 369, 372, 2 L. Ed. 2d 848, 851, 78 S. Ct. 819, 820-21 (1958) (police inducement short of entrapment is acceptable because "[c]riminal activity is such that stealth and strategy are necessary weapons in the arsenal of a police officer"); United States v. Peters, 153 F.3d 445, 464 (7th Cir. 1998) (Easterbrook, J., concurring) ("Deception plays an important and legitimate role in law enforcement"); People v. Zamora, 940 P.2d 939, 942 (Colo. App. 1996) (collecting cases in which police deception leading to consent deemed fair or consent deemed voluntary); see also Model Penal Code, §2.13, comment 2 (1985) (regarding entrapment, "some tactics employing misrepresentation and persuasion are necessary to successful police work and ought not to be forbidden").

The Supreme Court resolved this ambiguity by providing a clearer definition of "voluntariness" in its decision in Schneekloth. There, the Supreme Court turned to the "judicial exposition of the meaning of 'voluntariness' " in the context of confessions to define the test for a suspect's consent. Schneekloth, 412 U.S. at 223, 36 L. Ed. 2d at 860-61, 93 S. Ct. at 2045-46. The Supreme Court observed that the voluntariness test in confession cases reflected the competing values implicated in police interrogation: "the need for police questioning as a tool for the effective enforcement of criminal laws" on one hand, and "society's deeply felt belief that the criminal law cannot be used as an instrument of unfairness, and that the possibility of unfair and even brutal police tactics poses a real and serious threat to civilized notions of justice" on the other. Schneekloth, 412

U.S. at 224-25, 36 L. Ed. 2d at 861, 93 S. Ct. at 2046. Because consent cases raise similar considerations, and because it reasoned that "the requirement of a 'voluntary' consent reflects a fair accommodation of the constitutional requirements involved," the Supreme Court held that "there [was] no reason *** to depart in the area of consent searches, from the traditional definition of 'voluntariness.'" Schneckloth, 412 U.S. at 229, 36 L. Ed. 2d at 864, 93 S. Ct. at 2049.² Under the test adopted in Schneckloth, a consent will be deemed involuntary and thus invalid where it is "coerced, by explicit or implicit means, by implied threat or covert force" (Schneckloth, 412 U.S. at 228, 36 L. Ed. 2d at 863, 93 S. Ct. at 2048) and is therefore not "the product of an essentially free and unconstrained choice" by the suspect (Schneckloth, 412 U.S. at 225, 36 L. Ed. 2d at 862, 93 S. Ct. at 2047). This assessment of voluntariness "is a question of fact to be determined from all the circumstances" (Schneckloth, 412 U.S. at 248-49, 36 L. Ed. 2d at 875, 93 S. Ct. at 2059) that takes into account both the characteristics of the accused and the details of the encounter (see Schneckloth, 412 U.S. at 226, 36 L. Ed. 2d at 862, 93 S. Ct. at 2047). In the time since Schneckloth, courts have developed a list of factors that might render a consent involuntary. Among those factors are "the defendant's age, education, and intelligence, the length of [any] detention and the duration of the

²Many authorities, including the majority, imply that courts must weigh the competing considerations identified in Schneckloth to determine whether a consent was voluntary (see slip op. at 13-14), but, as the above discussion indicates, the Supreme Court actually considered those factors itself before adopting the definition of voluntariness previously used only in confession cases. The dueling considerations are thus already "reflect[ed]" (Schneckloth, 412 U.S. at 229, 36 L. Ed. 2d at 864, 93 S. Ct. at 2048-49) in the Supreme Court's voluntariness test and should not be considered anew.

questioning, whether the defendant was advised of his constitutional rights, and whether the defendant was subjected to any physical mistreatment." People v. Spann, 332 Ill. App. 3d 425, 439 (2002).³

In the time since Schneckloth, lower courts have applied the voluntariness test to police deception cases with inconsistent results. It is widely acknowledged that police deception could work to coerce an involuntary consent in the way Schneckloth forbids, by interfering with the suspect's ability to make a free choice to grant or deny consent. For example, in Bumper, a case that predates Schneckloth but is nonetheless instructive, the Supreme Court held invalid a consent procured by a police officer falsely telling a suspect that he possessed a search warrant, because the consent was coerced by the officer's announcing "in effect that the [suspect] ha[d] no right to resist the search." Bumper, 391 U.S. at 550, 20 L. Ed. 2d at 803, 88 S. Ct. at 1792. The majority cites Bumper along with a series of Illinois cases in which police undermined the suspects' free will by falsely asserting that they could seize the property to be searched in the absence of consent (Casazza, 144 Ill. 2d 414) or by making unsupportable threats against the suspects' property (Bailey, 273 Ill. App. 3d 431) or family (Purchase, 214 Ill. App. 3d 152). Each of these types of deception works somehow to rob the suspect of the sense of free choice to grant or deny consent, either by leaving the suspect with the impression that the law or the circumstances allow no choice or by conveying

³Even after Schneckloth, there is some federal authority invoking federal courts' supervisory power to strike, in the interest of fairness, a consent obtained through police deception. See Securities & Exchange Commission, 645 F.2d at 317. The Illinois Appellate Court does not enjoy the same supervisory power, and I therefore do not consider the propriety of this basis for invalidating a consent.

a threat that tends to undermine the suspect's will to refuse. It therefore makes sense that a consent given in the face of these types of police deception should not be considered voluntary.

Some cases, however, have expanded the rule against these types of deception into a blanket prohibition of all deception leading to consent. These courts have held, without qualification, that " 'consent obtained through deception cannot be said to have been given freely and voluntarily.' " State v. Hickson, 69 Ohio App. 3d 278, 280, 590 N.E.2d 779, 780 (1990), quoting State v. Pi Kappa Alpha Fraternity, 23 Ohio St. 3d 141, 144, 491 N.E.2d 1129, 1132 (1986). Other courts have implied the same rule by indiscriminately equating all types of deception with unconstitutional coercion (Graf, 265 Ill. App. 3d at 750 ("[c]onsent is not voluntary where it is the result of official coercion, intimidation, or deception")) or by stating the same rule with the meager qualification that deception invalidates consent "if the consent was given in reliance on" the misrepresentation. United States v. Briley, 726 F.2d 1301, 1304 (8th Cir. 1984); United States v. Turpin, 707 F.2d 332, 335 (8th Cir. 1982). (These statements from the Eighth Circuit cases rely on Bumper as authority, but I have described the reach of Bumper above as being more limited than the statements suggest.) Some cases thus hold that consent will be involuntary where the police tell a suspect that they wish to enter her home to look out her window when they actually expect to see illegal drugs in plain view upon entry (Hickson, 69 Ohio App. 3d 278, 590 N.E.2d 779), while others imply that an officer's misleading a suspect as to whether he is the subject of an investigation could render involuntary a consent to search (Turpin, 707 F.2d at 335 (noting that police had misled the defendant but further noting that police had supplied information that "clearly implied" the defendant was a suspect and that police did not misrepresent their legal authority to search)).

I disagree with the per se rule that can be drawn from these cases. See Peters, 153 F.3d at 463 (Easterbrook, J., concurring) ("A statement's voluntariness is not undercut by the fact that the

speaker was unaware that he was a target"). It does not follow that, because some types of police deception can render a consent involuntary, all types of police deception should invalidate consent. This notion is decidedly inconsistent with the Supreme Court's ubiquitous admonition that courts evaluate the totality of the circumstances in making this type of assessment, and it expands the prohibition on police deception far beyond the voluntariness test announced in Schneekloth. See 4 W. LaFare, Search & Seizure §8.2(n), at 136-37 (4th ed. 2004) ("But, at least since Schneekloth v. Bustamonte, it cannot be said that such deception is inherently incompatible with consent, for in Schneekloth the Court adopted the voluntariness test from the coerced confession cases, which has not been deemed to compel the exclusion of statements obtained by police misrepresentation of the crime under investigation"); see also People v. Martin, 102 Ill. 2d 412, 427 (1984) (police deception "does not invalidate [a] confession as a matter of law").

It is also inconsistent with the realities of police work, which often involves undercover investigations of the type that would not be allowed under a per se rule against deception leading to consent. The Supreme Court has endorsed such undercover police work in the face of a challenge that it constituted deception invalidating consent. In Lewis v. United States, 385 U.S. 206, 17 L. Ed. 2d 312, 87 S. Ct. 424 (1966), a federal agent posed as a drug buyer and was admitted into the defendant's home, where he purchased drugs. The Supreme Court noted that the defendant "invited the undercover agent to his home" and that the agent did not "see, hear, or take anything that was not contemplated, and in fact intended, by [the defendant] as a necessary part of his illegal business." Lewis, 385 U.S. at 210, 17 L. Ed. 2d at 315-16, 87 S. Ct. at 427. After Lewis, there can stand no per se rule forbidding police deception leading to consent.

I include one important side note. The Supreme Court in Lewis went on to say that, "when *** the home is converted into a commercial [business] center to which outsiders are invited for

purposes of transacting unlawful business," a government agent, "in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant." Lewis, 385 U.S. at 211, 17 L. Ed. 2d at 316, 87 S. Ct. at 427. Although some have argued based on this language that the Supreme Court's decision should be limited to instances in which the undercover agent participates in an illegal venture, or that it should be limited to business or commercial ventures, other cases have dispensed with this proposed distinction. For example, in State v. Poland, 132 Ariz. 269, 645 P.2d 784 (1982), the Arizona Supreme Court ruled constitutionally acceptable an FBI agent's posing as a prospective home buyer to gain entry into a home, where he found incriminating evidence in plain view. The court cited Lewis along with several cases in which law enforcement officers concealed their identity in order to gain consent and then held that "[t]he only limitation appears to be that the agent is limited to conduct which would be normal for one adopting the disguise used in seeking entry." State v. Poland, 132 Ariz. at 277, 645 P.2d at 792, citing United States v. Ressler, 536 F.2d 208 (7th Cir. 1976) (agents posing as potential buyers to investigate firearms), United States v. Glassel, 488 F.2d 143 (9th Cir. 1973) (agents posing as potential narcotics buyers), State v. Sardo, 112 Ariz. 509, 543 P.2d 1138 (1975) (agents posing as hotel managers), United States v. Raines, 536 F.2d 796 (8th Cir. 1976) (law enforcement posing as an acquaintance), United States v. Wright, 641 F.2d 602 (8th Cir. 1981) (law enforcement posing as a motorist with car trouble), and United States v. Bullock, 590 F.2d 117 (5th Cir. 1979) (law enforcement posing as a potential Ku Klux Klan member); see also Guidry v. State, 671 P.2d 1277, 1281 (Alaska 1983) (rejecting distinction between police participation in legal and illegal activity); State v. Stevens, 123 Wis. 2d 303, 315, 367 N.W.2d 788, 794-95 (1985) (applying Lewis rule to a police officer posing as a garbage collector but doing nothing defendant did not contemplate a garbage collector would do). Because there is no question

that defendant here knew that he was dealing with police, I do not address the effect of police deception as to their identity as police. My discussion herein is confined to the question of police deception as to their purpose for requesting consent.

Other cases do not support a rule that police deception per se renders a consent to search involuntary but instead include deception among the factors to be included in the voluntariness assessment. E.g., Minniti, 373 Ill. App. 3d at 69; Zamora, 940 P.2d at 942. (The majority here adopts the factor approach while simultaneously endorsing the per se approach implied in Graf.) These cases are correct, but, by failing to warn that courts must discriminate between those types of deception that undercut free will and those that do not, they leave the potential for misunderstanding. The presence of police deception becomes a factor in assessing voluntariness only when the deception is actually coercive in the sense that it undercuts the free will of the consenting party.

With the above understanding of voluntariness, I see nothing to indicate that any police deception in this case interfered with the voluntariness of defendant's consent. Before addressing this issue, I must clarify the facts informing it. The parties, the trial court, and the majority mischaracterize Detective Smith's testimony describing the nature of his investigation. Smith testified that he was investigating credit card fraud when he went to defendant's home, but, by that testimony, he did not indicate that he was investigating only credit card fraud and not child pornography. Rather, the import of his testimony was that he had received a tip that defendant's credit card had been used to gain access to child pornography, but, due to suspicious activity on the credit card account and the fact that the card had been used only sparingly for child pornography purchases, he had yet to determine conclusively that defendant was the person who used the card and was not an innocent victim of credit card fraud. Defendant wrongly casts Smith's testimony as raising the incredible assertion that Smith was pursuing only a credit card fraud investigation, and

the majority repeats the error by saying that Smith "claimed he was investigating credit card fraud and not child pornography when he sought" consent to search defendant's computer. Slip op. at 13. The majority further perpetuates the misunderstanding by reciting that Smith "admitted" various connections between his investigation and suspicion of defendant's purchase of Internet child pornography. Slip op. at 7. Read properly, the whole of Smith's testimony is consistent with his "admissions" that he was investigating child pornography.

From this, and from Smith's and defendant's testimony that Smith made no mention to defendant of the child pornography investigation, it becomes manifest that Smith withheld a major, and likely driving, purpose of his request to search. However, there is little to indicate that Smith's concealing his primary purpose did anything to alter the voluntariness of defendant's consent to allow the search of his computer.⁴ The only aspect of the alleged police deception that could have affected the voluntariness of defendant's consent was its tendency to imply that defendant's personal information might have been imperiled until police were able to examine his computer. See United States v. Parson, No. 3:2007--10, slip op. at 13 (W.D. Pa. February 25, 2009) (discussing the coercive effect of the "specter of identity theft"). However, defendant undermined this possibility

⁴There is of course a possibility that defendant would have refused consent if he had known that the officers were actually looking for illegal images, but, as the above discussion demonstrates, that is not the test for voluntariness. In many of the cases discussed above, the defendant unquestionably would not have granted consent had police not deceived him, but the courts nonetheless deemed the consent voluntary. See e.g., Lewis, 385 U.S. 206, 17 L. Ed. 2d 312, 87 S. Ct. 424 (consent to allow undercover agent posing as drug purchaser into home not deemed involuntary).

by testifying that he was confident in the security of his computer and that he granted consent only because "it can't hurt to have [the police] look at [his] computer" with their purportedly stronger virus detection software. Therefore, although I disagree with the majority's inconsistent descriptions of the legal significance of police deception, I agree with the majority that any deception here did not render defendant's consent involuntary.

The next question is whether the police exceeded the scope of defendant's consent by viewing the images on his computer. Like the standards for voluntariness of consent, the standards for defining the scope of consent have developed over time. At one time, a plurality of the United States Supreme Court held that police conducting a search pursuant to a warrant (or an exception to the warrant requirement) could seize items found in plain view during the search but not identified in the warrant (or used to justify an exception to the warrant requirement) only where the discovery of the items was "inadvertent." Coolidge v. New Hampshire, 403 U.S. 443, 469, 29 L. Ed. 2d 564, 585, 91 S. Ct. 2022, 2040 (1971). Thus, under the plurality opinion in Coolidge, "[i]f the initial intrusion [was] bottomed upon a warrant that fail[ed] to mention a particular object, though the police [knew] its location and intend[ed] to seize it, then there [was] a violation" of the fourth amendment. Coolidge, 403 U.S. at 471, 29 L. Ed. 2d at 586, 91 S. Ct. at 2040-41. However, in Horton v. California, 496 U.S. 128, 110 L. Ed. 2d 112, 110 S. Ct. 2301 (1990), the Supreme Court overruled the Coolidge plurality and discarded the "inadvertence" requirement. Thus, in Horton, an officer who sought to find weapons and proceeds of a robbery, but obtained a warrant allowing a search only for the proceeds, did not violate the fourth amendment by seizing weapons when he found them in plain view during his search for the proceeds.

The holding in Horton brought cohesion to fourth amendment jurisprudence, which measures the scope of a consent to search not in terms of the subjective intentions, understandings, or

expectations of the parties involved but, rather, by an objective standard that asks what the "typical reasonable person" would have "understood by the exchange between the officer and the suspect." Florida v. Jimeno, 500 U.S. 248, 252, 114 L. Ed. 2d 297, 303, 111 S. Ct. 1801, 1804 (1991); People v. Ledesma, 206 Ill. 2d 571, 593 (2003).

The majority nonetheless invokes a rule that would bind police to the stated purpose of their search and forbid consensual searches for undisclosed purposes. The majority bases its rule on a misreading of our supreme court's statement that "the parameters of a search are usually defined by the purpose of the search" (James, 163 Ill. 2d at 314). This was the same erroneous approach adopted by the court in Richardson, 583 F. Supp. 2d 694, a closely analogous case upon which the majority relies as persuasive authority. See Richardson, 583 F. Supp. 2d at 713 (reaching same result by relying on Supreme Court's statement that "[t]he scope of a search is generally defined by its expressed object' "), quoting Jimeno, 500 U.S. at 251, 114 L. Ed. 2d at 303, 111 S. Ct. at 1804. However, just as police, when executing a search based on a warrant or on probable cause to search for a particular item, may hope to find additional items so long as they do not expand or change the scope or increase the intensity of the search (Horton, 496 U.S. 128, 110 L. Ed. 2d 112, 110 S. Ct. 2301), police executing a consensual search need not hew absolutely to the stated purpose of the search, so long as their search does not deviate from the scope or exceed the intensity of the search to which the suspect consented. The passage upon which the majority (and Richardson) relies derives from the Supreme Court's opinion in People v. Ross, 456 U.S. 798, 72 L. Ed. 2d 572, 102 S. Ct. 2157 (1982), which offers the proper context for the statement:

"The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just

as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the truck of a taxi contains contraband or evidence does not justify a search of the entire cab." Ross, 456 U.S. at 824, 72 L. Ed. 2d at 593, 102 S. Ct. at 2172.

In Jimeno, the Supreme Court applied this concept in a consent-to-search case:

"The scope of a search is generally defined by its expressed object. United States v. Ross, 456 U.S. 790, 102 S. Ct. 2157, 72 L. Ed. 2d 572 (1982). In this case, the terms of the search's authorization were simple. Respondent granted [law enforcement] permission to search his car, and did not place any explicit limitation on the scope of the search. [The officer] had informed respondent that he believed respondent was carrying narcotics, and that he would be looking for narcotics in the car. We think that it was objectively reasonable for the police to conclude that the general consent to search respondent's car included consent to search containers within that car which might bear drugs." Jimeno, 500 U.S. at 251, 114 L. Ed. 2d at 303, 111 S. Ct. at 1804.

The principle to be drawn from these cases is not that an officer may have no purpose for a consent search ulterior to his stated purpose, but instead that a description of the purpose of a search can serve as an indicator of the scope of the contemplated search and thus can help define the scope of the consent. The restriction on the search comes not from the stated purpose of the search, but from what a reasonable person would have understood the extent of the consent to be--i.e., what areas a reasonable person would have understood police had been granted authority to search. Courts say that the scope of a search generally is defined by its purpose because the stated purpose

of a proposed search will often be the only explanation of the scope of the proposed search: the scope of a consent to a "search for drugs" without further explanation will be understood in those terms. Thus, police who describe a proposed automobile search by telling the suspect that they wish to search for liquor will have limited the scope of their search to places where liquor could be found, but any other contraband found in the course of that search may still lawfully be seized. People v. Andeliz, 3 Misc. 3d 384, 389, 773 N.Y.S.2d 853, 858 (2004). Or, police who tell a suspect that they intend to search for weapons when they actually expect to find drugs may still seize drugs during their search, because "such a statement on the part of [law enforcement] could [not] affect the validity of [the suspect's] consent, the area to be searched being identical in either event." Pupo v. State, 187 Ga. App. 765, 767, 371 S.E.2d 219, 222 (1988). Or, police who ask to search a suspect's bag for drugs, when they actually expect to find stolen money and jewelry, do not exceed the scope of the suspect's consent. United States v. White, 706 F.2d 806, 808 (7th Cir. 1983);⁵ see also W. LaFave, Search & Seizure §8.2, at 136 n.378 (4th ed. 2004) (collecting cases).

Even though the court in Richardson overlooked this distinction and misread the law in the same way the majority now misreads it, the facts of the case provide a clear illustration of the point. In Richardson, law enforcement agents investigating child pornography that was charged to the defendant's credit card implied to the defendant that they suspected he was the victim of identity theft, and on that basis the defendant granted them consent to make duplicates of his hard drives and then look at the duplicates. Richardson, 583 F. Supp. 2d at 700-01, 702. The stated purpose of the search in Richardson was to look at the hard drives to determine if the defendant's personal

⁵During oral argument in the current case, I proposed to defense counsel a hypothetical question based on White, but I received no direct answer.

information had been compromised, but the defendant consented to a search of the entirety of his hard drives. The terms of the defendant's consent, and not the purpose of the search, should have defined the law enforcement agents' authority to search. Since the consent to search the hard drives was unlimited, the agents' eventual search for illegal images on the hard drive did not exceed the scope of the consent. However, as noted, the court in Richardson reached the opposite result based on the misunderstanding of Jimeno that I repudiate above.

Before applying the above principles to determine whether the search conducted in this case exceeded the scope of the consent conferred, I must again clarify some pertinent facts. As I note above, the permissible scope of a search is governed not necessarily by its stated purpose, but instead by what a reasonable person would have understood from the exchange precipitating the consent search. It therefore becomes very important to determine precisely how Smith and defendant described the requested search before defendant assented. The testimony is ambiguous on this point. It is true, as the majority and the parties note, that Smith told defendant that his purpose in searching the computer was to look for malware. However, the testimony does not include any description of how Smith described to defendant the process by which he would search the computer for malware. The majority seems to assume from this gap in the testimony that the only description given was that Smith would perform a "virus search," and the majority therefore repeats or implies several times that the scope of the consent was limited accordingly. See slip op. at 19 ("Here, Detective Smith, by his own words, limited the scope"); slip op. at 20 ("Defendants have the right to place explicit limitations on the scope of their consent"); slip op. at 21 ("Defendant's failure to object *** did not serve to transform his original limited consent"); slip op. at 21 ("If Detective Smith wanted a general consent from defendant, he should have refrained from including limitations in his request"). I disagree with the majority's assumption.

Although the testimony does not directly state what Smith and defendant discussed prior to defendant's consent, it does provide clues. When asked to describe how he would search defendant's computer for malware, Smith described using an "image scan" program that boots the computer in a read-only mode and then calls up all of the images on the computer. The majority and the parties incorrectly imply that Smith testified that he examined the images themselves for signs of malware, but in his testimony Smith actually described differently the connection between the image scan and the search for malware. Smith said that he used the program to search for viruses because the program revealed the origin of each of the images, and, for those images originating from Web sites, Smith could ask defendant if he recalled visiting the sites. According to Smith, "[i]f someone [was] accessing his computer remotely unbeknownst to him, he [could] tell [Smith] then and there" that he had not visited the sites. Smith said that he focused his search on images portraying credit card logos, because such images often appear on Web pages that collect credit card numbers for purchases.

The efficacy of this "image viewing" technique as a virus search, especially when compared to the type of actual virus search Smith testified he forwent in order to do the image search, is questionable--a point with which the majority appears to agree. See slip op. at 19-20 (relying on defendant's testimony that "no image would lead Detective Smith to discover a virus").⁶ However, the issue here is not whether Smith pursued a search that would reveal viruses but, rather, whether he pursued a search consistent with the scope of the consent he had obtained, i.e., consistent with

⁶The majority does not explain how its statement that the image scan program cannot have been used to detect a virus (slip op. at 19-20) can be squared with its conclusion that Smith did not employ "trickery, deceit, or subterfuge" in obtaining consent (slip op. at 16).

what a reasonable person would have understood as the scope of the consent defendant granted.

Smith's testimony contains the following passage:

"Q. And when you asked him to view his--when you asked about his computer, was that your intent to try and use those programs?

A. Yes, sir.

Q. And did you, in fact, inform the defendant of that?

A. Yes sir."

In the absence of testimony that directly relates how Smith described the program to defendant before defendant agreed to the search, Smith's description of the image scan program as a tool for detecting malware, convincing or not, gives us insight into the conversation referenced in his testimony.

Defendant's actions after the image search began provide added insight into what the two men discussed before defendant granted consent. Smith testified that defendant was in the room when Smith started the image scan program, watched as Smith conducted a review of the images on the computer, and continued to talk to Smith as Smith ran the program, yet never asked Smith to stop viewing the pictures. In his own testimony, defendant confirmed that he was with Smith when Smith began looking at images on the computer, and he testified that he raised no objection even though he actually commented (before Smith found the illegal pornographic images) that he was embarrassed of the other (legal pornographic) images Smith had uncovered on the computer. While it is true, as the majority notes, that a defendant's silence cannot be used to transform the original scope of the consent (slip op. at 21), it can provide an indication that the search was within the scope of the consent. United States v. Gordon, 173 F.3d 761, 766 (10th Cir. 1999) ("We consistently and repeatedly have held a defendant's failure to limit the scope of a general authorization to search, and

failure to object when the search exceeds what he later claims was a more limited consent, is an indication the search was within the scope of consent").

From the above, I infer that Smith discussed the image scan program with defendant before defendant granted consent, and, even if I were to conclude that Smith misled defendant as to the purpose of using the program, I would conclude that Smith's use of the program fell within the scope of the consent.

Based on the above discussion, I would hold that the search of defendant's computer for images did not exceed the scope of defendant's voluntary consent, and I would affirm defendant's conviction.