Chapter 7

CONSENT SEARCHES; COMPELLING DISCLOSURE OF PASSWORDS

This chapter addresses the validity of consent to search computers — a Fourth Amendment issue — and addresses compelling a suspect to disclose his password or encryption key — a Fifth Amendment issue.

§ 7.1 CONSENT — IN GENERAL

The principles regulating the permissibility of a search or seizure based on a claim of consent do not change in the context of computer and other digital evidence searches.[1] However, computers and digital evidence searches present several challenges to the application of those principles.

Consent to search is a question of fact and is determined based on the totality of the circumstances.[2] The ultimate question turns on the voluntary nature of the consent.[3] A person may "delimit as he chooses the scope of the search to which he consents."[4] The government, in performing a search, cannot exceed the scope of the consent given. This is an objective inquiry: "what would the typical reasonable person have understood by the exchange between the officer and the suspect?"[5] Moreover, the scope of a consensual search is generally defined by its expressed object.[6] This is to say that consent "extends to the entire area in which the object

---

[1] *See, e.g.*, United States v. Mabe, 330 F. Supp. 2d 1234 (D. Utah 2004) (rejecting assertion that defendant consented to search of computer after police falsely stated that they had search warrant); People v. Yuruckso, 746 N.Y.S.2d 33, 34-35 (N.Y. App. Div. 2002) (consent to search home computer valid, based on defendant's maturity, education, and other factors, even though police stated that, if he did not consent, they would obtain a search warrant and seize his work computer).

[2] Ohio v. Robinette, 519 U.S. 33 (1996).

[3] *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). Voluntariness — meaning the lack of coercion by the government agents — must be established. However, the consent need not be an informed one, which is to say that the person giving the consent need not know that he or she has the right to refuse, which is the essential holding of *Schneckloth*.

[4] Florida v. Jimeno, 500 U.S. 248, 252 (1991). *Cf.* United States v. Lemmons, 282 F.3d 920, 924-25 (7th Cir. 2002) (although suspect gave limited consent initially, his later consent to search computer made search valid).

[5] Florida v. Jimeno, 500 U.S. 248, 251 (1991).

[6] *Id. See also* United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003) (seizure of "homemade" adult pornography within scope of consent to search for "'materials [that] are evidence in the nature of' child abuse, child erotica, or child exploitation" as it showed ability and intent to manufacture pornography depicting himself in sexual acts); United States v. Turner, 169 F.3d 84, 88-89 (1st Cir. 1999) (scope of defendant's permission to search apartment in connection with intruder's assault on neighbor exceeded when police accessed files on his computer because the police request would have been reasonably

of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."[7]

For example, when a graduate student in computer science agreed to allow agents to search his entire home and to take his computer back to the FBI office for further examination, it was held that the student "would have realized that the examination of his computer would be more than superficial when the agents explained that they did not have the skills nor the time to perform the examination in his home."[8] Moreover, according to the court, "a graduate student in computer science would clearly understand the technological resources of the FBI and its ability to thoroughly examine his computer." Given the lack of limitations put on the search by the student, his cooperation, and his expertise, the court believed it was reasonable for the agents to conclude that they had unlimited access to the computer.

---

§ 7.2 CONSENT — SCOPE ISSUES

PEOPLE v. ROBERT S. PRINZING
907 N.E.2d 87 (Ill. Ct. App. 2009)

JUSTICE BOWMAN delivered the opinion of the court.

Robert S. Prinzing was convicted of possessing child pornography. He 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.

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

---

understood to be that they intended to search for physical evidence of the assault); State v. Brown, 813 N.E.2d 956, 960 (Ohio Ct. App. 2004) (scope of defendant's consent exceeded when police seized two computers from his home when he had merely given consent to look at computers).

[7] United States v. Ross, 456 U.S. 798, 820-21 (1982). *See also* Florida v. Jimeno, 500 U.S. 248, 251 (1991) (consent to search car included closed paper bag on floor of car); Commonwealth v. Hinds, 768 N.E.2d 1067, 1071 (Mass. 2002) (when defendant consented to search of his computer for electronic mail, valid search not limited to specific directories or locations on computer).

[8] United States v. Al-Marri, 230 F. Supp. 2d 535, 539-40 (S.D.N.Y. 2002).

Detective Grimes, went to defendant's residence. 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. 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.

On cross-examination, Detective Smith admitted [, *inter alia*,] that he was specifically assigned to review cases that involved Internet child pornography [and that he was investigating the defendant for possession of child pornography].

Defendant testified. 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.

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.

[After first determining] that defendant's consent was voluntary, we now examine whether the police exceeded the scope of the consent. 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. "[T]he parameters of a search are usually defined by the purpose of the search."

In this case, principles of law and technology collide. The court in *People v. Berry*, 731 N.E.2d 853 (Ill. App. 2000), addressed the scope of consent with respect to electronic devices, specifically a cellular phone. 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. 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. 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.'" The officer, after receiving the defendant's response, opened the phone and retrieved the phone number of the phone by pressing a button. 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. 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.

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. The officers then opened images saved on the computer that were pornographic images of children. 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. Because the defendant did not limit the consent to search his computer, the police did not exceed the scope by searching random images.

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. 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. 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.

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.

JUSTICE O'MALLEY, dissenting:

The . . . question is whether the police exceeded the scope of defendant's consent by viewing the images on his computer.

The principle to be drawn 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 the 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. 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."

It 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. 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. 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 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. While it is true that a defendant's silence cannot be used to transform the original scope of the consent, it can provide an indication that the search was within the scope of the 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.

NOTES

What is the permissible scope of a search of a computer for "viruses?" Is that a technical question? Is looking at logos within the scope of such a search?

---

1. Scope: Does consent to search include forensic exam?

UNITED STATES v. JONATHAN LUKEN
560 F.3d 741 (8th Cir. 2009)

Melloy, Circuit Judge.

An Immigration and Customs Enforcement investigation revealed that two credit card numbers believed to be Luken's were used in 2002 and 2003 to purchase child pornography from a website in Belarus. On July 25, 2006, three law-enforcement officers visited Luken at his place of employment. One of the officers, Agent Troy Boone of the South Dakota Department of Criminal Investigation, informed Luken that the officers believed Luken's credit card had been used to purchase child pornography. Boone told Luken that the officers wanted to speak with Luken

privately about the matter and look at his home computer. Luken agreed to speak with them at his home and drove himself to his house to meet them.

Upon arriving at Luken's home, Luken allowed the officers to enter his house. Luken's wife was home, so Boone offered to speak with Luken privately in Boone's car. Luken agreed. Once inside the car, Boone informed Luken that Luken did not have to answer any questions, was not under arrest, and was free to leave. Luken nevertheless agreed to speak with Boone. Luken discussed the nature of his computer use and knowledge. He admitted to purchasing and downloading child pornography for several years. He also admitted to looking at child pornography within the previous month. He stated, however, that he believed he had no child pornography saved on his computer.

After Luken admitted to viewing child pornography, Boone asked Luken if officers could examine Luken's computer. Boone explained the nature of computer searches to Luken and told Luken that, even if files had been deleted, police often could recover them with special software. Boone asked Luken if a police search would reveal child pornography in Luken's deleted files. Luken stated that there might be "nature shots" on his computer, i.e., pictures of naked children not in sexually explicit positions, that he recently viewed for free. Boone then asked Luken to consent to a police search of Luken's computer, and Boone drafted a handwritten consent agreement stating, "On 7-25-06, I, Jon Luken, give law enforcement the permission to seize & view my Gateway computer." Luken signed and dated the agreement.

[The police seized the computer and Boone later] used forensic software to analyze it. Boone discovered approximately 200 pictures he considered child pornography.

The question before us is whether it was reasonable for Boone to consider Luken's consent to seize and "view" his computer to include consent to perform a forensic analysis on it. We believe it was.

Before Luken consented to police seizing and viewing his computer, Luken initially had told Boone that Luken believed there was no child pornography saved on his computer. Boone, however, explained to Luken that police could recover deleted files using special software. Boone then specifically asked Luken if such a search would reveal child pornography on Luken's computer. Luken responded that there probably would be such material on his computer and stated that police might find "nature shots" if they did such a search. At that point, Luken gave Boone permission to seize and view his computer without placing "any explicit limitation on the scope of the search."

Given the above-described exchange, we agree with the district court that a typical reasonable person would have understood that Luken gave Boone permission to forensically examine Luken's computer. Boone made it apparent to Luken that police intended to do more than merely turn on Luken's computer and open his easily accessible files. Boone explained that police possessed software to recover deleted files and asked Luken specifically if such software would reveal child pornography on Luken's computer. Luken responded by telling Boone that such a search would likely reveal some child pornography. He then gave Boone permission to seize and view the computer. In that context, a typical reasonable person would

understand the scope of the search that was about to take place. Therefore, because we affirm the district court's finding that Luken consented to the search, we hold there were no Fourth Amendment violations.

---

2. Cell Phones: Scope of Consent

JERMAINE L. SMITH v. STATE
713 N.E.2d 338 (Ind. Ct. App. 1999)

KIRSCH, JUDGE.

Smith appeals his conviction of theft, for using a "cloned" cellular telephone reprogrammed to have an internal electronic serial number ("ESN") different than its external ESN. Put in the vernacular, Smith was convicted of using an illegal cellular phone which had been modified such that, when in use, the charges would be billed to someone else's active cellular phone number.

Indiana State Police Sergeant David Henson pulled over a blue and white Oldsmobile driven by Steve Martin, in which Smith was a front seat passenger. Trooper Henson initiated the traffic stop because a computer check on the vehicle's license plate revealed the plate was registered to a yellow Oldsmobile rather than a blue and white one. Trooper Henson approached the vehicle and asked Martin for his license and registration. Following the arrival of Troopers Troy Sunier and Patrick Spellman, Martin and Smith were asked to exit the vehicle, separated, and questioned in an effort to determine if the car was stolen. The troopers' inquiries revealed that the car belonged to Smith, who had painted it a different color, which explained the apparently mismatched license plate.

During the course of this investigatory stop, Trooper Dean Wildauer arrived on the scene and asked Smith if he and Trooper Spellman could search the vehicle for guns, drugs, money, or illegal contraband. Smith consented to the search. While no guns, drugs, money, or illegal contraband were recovered as a result of the search, two cellular flip phones were retrieved from the front seat of Smith's car. One phone was found on the passenger's side of the vehicle where Smith had been sitting, and the other was found on the driver's side where Martin had been sitting. When asked whether the cellular phone found on the passenger's side was his, Smith stated that it was his girlfriend's; however, he could not recall the name of her service provider.

Trooper Wildauer then took both phones back to his police vehicle where he removed the batteries and performed a short-out technique on each device. The results of this field-test revealed that the cellular phones' internal ESNs did not match the external ESNs, indicating that the cellular phones had been illegally cloned, or reprogrammed such that, when in use, the charges would be billed to someone else's phone number. After discovering that the phones were cloned, Trooper Wildauer called a law enforcement hotline which informed him that the internal ESN of the cellular phone Smith claimed was his girlfriend's in fact belonged to GTE Mobilnet and was assigned to one of its legitimate service

customers, Technology Marketing Corporation. Upon further questioning, Smith admitted that he had purchased the cloned phone on the street from an acquaintance and that he knew it was a clone.

Initially, we observe that Sergeant Henson's investigatory stop of Smith's vehicle was valid and supported by reasonable suspicion. There are no such indicators here that Smith's consent was in any way induced by fraud, fear, or intimidation. Under the totality of these circumstances, we conclude that Smith's consent to search his vehicle was voluntarily given.

Having held that Smith's consent to search was not constitutionally defective, we must then determine whether the troopers exceeded the scope of his consent. The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of objective reasonableness, in other words, "what would the typical reasonable person have understood by the exchange between the officer and the suspect?" In addition, the scope of a consensual search is generally defined by its expressed object.

Here, the expressed objects of the troopers' search were guns, drugs, money, or illegal contraband. When Smith gave the troopers permission to search his car for guns, drugs, money, or illegal contraband, a reasonable person would have understood Smith's consent to include permission to search any containers inside the vehicle which might reasonably contain those specified items. A cellular phone is a container capable of hiding such items as drugs or money. Therefore, it was proper for the troopers to seize the cellular phone long enough to determine whether it was truly an operating cellular phone or merely a pretense for hiding the expressed objects of their search.

Smith's consent did not authorize the troopers to access the computer memory of his cellular phone — an objectively reasonable person assessing in context Smith's verbal exchange with the troopers would have understood that the troopers intended to search only in places where Smith could have disposed of or hidden the specific items which they were looking for, namely, guns, drugs, money or other contraband. No objective person would believe that by performing a short-out technique on a cellular phone to retrieve its electronic contents, the troopers might reasonably find the expressed object of their search. Thus, where the troopers here obtained consent to search Smith's car for guns, drugs, money, or contraband, they had to limit their activity to that which was necessary to search for such items.

§ 7.3 THIRD PARTY CONSENT

The validity of third party consent depends on whether the person giving consent has either actual authority or apparent authority to consent.[9] In general, a third party may consent to a warrantless search when that party possesses "common authority over or other sufficient relationship to the premises or effects sought to be inspected."[10]

---

[9] *See, e.g.*, United States v. Smith, 27 F. Supp. 2d 1111, 1115 (C.D. Ill. 1998).

[10] United States v. Matlock, 415 U.S. 164, 171 (1974). *See also* Frazier v. Cupp, 394 U.S. 731, 740 (1969) (rejecting inquiry into "metaphysical subtleties" of argument that, because joint user of duffle bag

> Common authority is . . . not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[11]

The issue frequently arises in the context of shared computer use. The question, as with consent generally, turns on the person's access or control of the computer, regardless of whether the person is a spouse,[12] parent,[13] other family member,[14] house mate,[15] bailee,[16] systems administrator,[17] or other third party,[18] such as a computer repair person.[19]

1. Passwords and Encryption

The presence of password-protected files is an important consideration in assessing a third party's authority to consent. By creating password-protected files, the creator "affirmatively" intends to exclude the joint user and others from

---

only had actual permission to use one compartment, he could not consent to search of whole bag).

[11] *Matlock*, 415 U.S. at 171 n.7.

[12] *See* Walsh v. State, 512 S.E.2d 408, 411-12 (Ga. Ct. App. 1999) (defendant's wife had authority to consent to search of computer that she purchased and was available for use by family).

[13] *See* People v. Blair, 748 N.E.2d 318, 324-25 (Ill. Ct. App. 2001) (father, who had no actual or apparent ownership of computer, could not validly consent to seizure of son's computer).

[14] *See* State v. Guthrie, 627 N.W.2d 401 (S.D. 2001) (son-in-law possessed common authority over computer and could validly consent to its seizure when he had unconditional access and control over it).

[15] *See* United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (housemate had authority to consent to search of defendant's computer, to which she had joint access and which was located in common area of house; alternatively, government agents reasonably believed housemate could consent to search).

[16] *See* United States v. James, 353 F.3d 606, 614-15 (8th Cir. 2003) (bailee, who agreed to store disks and who had been later directed to destroy them, did not have actual or apparent authority to permit police to take and examine them).

[17] A systems administrator is the person "whose job is to keep [a computer] network running smoothly, monitor security, and repair the network when problems arise." U.S. Dep't of Justice, Searching and Seizing Computers and Electronic Evidence in Criminal Investigations 25 (3d ed. 2009). Those administrators "have 'root level' access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems." *Id.* Whether a systems administrator "may voluntarily consent to disclose information from or regarding a user's account varies based on whether the network belongs to a communications service provider, a private business, or a government entity." *Id.*

[18] *See* United States v. Meek, 366 F.3d 705, 711 (9th Cir. 2004) ("Like private phone conversations, either party to a chat room exchange has the power to surrender each other's privacy interest to a third party.").

[19] United States v. Barth, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (computer repair person did not have actual authority to consent to search of customer's hard drive, having "possession of the unit for the limited purpose of repair" and did not have apparent authority when police knew his status).

the files.[20] Under such circumstances, it has been reasoned, it cannot be said that the person has assumed the risk that the joint user would permit others to search the files.[21] On the other hand, the lack of passwords to protect files has been held to defeat a claim that the defendant had exclusive control of a computer and that his housemate did not have authority to consent to search.[22]

UNITED STATES v. RAY ANDRUS
483 F.3d 711 (10th Cir. 2007)

Murphy, Circuit Judge.

Federal authorities first became interested in Ray Andrus during an investigation of Regpay, a third-party billing and credit card aggregating company that provided subscribers with access to websites containing child pornography. The investigation of Regpay led to an investigation of Regpay subscribers. One of the subscribers providing personal information and a credit card number to Regpay was an individual identifying himself as "Ray Andrus" at "3208 W. 81st Terr., Leawood, KS." The Andrus Regpay subscription was used to access a pornographic website called www.sunshineboys.com. Record checks with the drivers license bureau and post office indicated Ray Andrus, Bailey Andrus, and a third man, Richard Andrus, all used the West 81st Terrace address. The credit card number provided to Regpay was determined to belong to Ray Andrus. The email address provided to Regpay, "bandrus@kc.rr.com," was determined to be associated with Dr. Bailey Andrus.

Eight months into the investigation, agents believed they did not have enough information to obtain a search warrant for the Andrus residence. They, therefore, attempted to gather more information by doing a "knock and talk" interview with the hope of being able to conduct a consent search. ICE Special Agent Cheatham and Leawood Police Detective Woollen arrived at the Andrus house at approximately 8:45 a.m. on August 27, 2004. ICE Special Agent Kanatzar, a forensic computer expert, accompanied Cheatham and Woollen to the residence, but waited outside in his car for Cheatham's authorization to enter the premises.

Dr. Andrus, age ninety-one, answered the door in his pajamas. Dr. Andrus invited the officers into the residence and, according to the testimony of Cheatham and Woollen, the three sat in Dr. Andrus' living room, where the officers learned that Ray Andrus lived in the center bedroom in the residence. In response to the officers' questions, Dr. Andrus indicated Ray Andrus did not pay rent and lived in the home to help care for his aging parents. Cheatham testified he could see the

---

[20] Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

[21] *Id*. *See also* United States v. Slanina, 283 F.3d 670, 676 (5th Cir.), *remanded on other grounds*, 537 U.S. 802 (2002), *on appeal after remand*, 359 F.3d 356 (5th Cir. 2004) (use of passwords and locking office doors to restrict employer's access to computer files is evidence of employee's subjective expectation of privacy in those files).

[22] United States v. Smith, 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998).

door to Ray Andrus' bedroom was open and asked Dr. Andrus whether he had access to the bedroom. Dr. Andrus testified he answered "yes" and told the officers he felt free to enter the room when the door was open, but always knocked if the door was closed.

Cheatham asked Dr. Andrus for consent to search the house and any computers in it. Dr. Andrus signed a written consent form indicating his willingness to consent to a premises and computer search. He led Cheatham into Ray Andrus' bedroom to show him where the computer was located. After Dr. Andrus signed the consent form, Cheatham went outside to summon Kanatzar into the residence. Kanatzar went straight into Andrus' bedroom and began assembling his forensic equipment. Kanatzar removed the cover from Andrus' computer and hooked his laptop and other equipment to it. Dr. Andrus testified he was present at the beginning of the search but left the bedroom shortly thereafter. Kanatzar testified it took about ten to fifteen minutes to connect his equipment before he started analyzing the computer. Kanatzar used EnCase forensic software to examine the contents of the computer's hard drive. The software allowed him direct access to the hard drive without first determining whether a user name or password were needed. He, therefore, did not determine whether the computer was protected by a user name or password prior to previewing the computer's contents. Only later, when he took the computer back to his office for further analysis, did he see Ray Andrus' user profile.[n.1][23]

Kanatzar testified he used EnCase to search for.jpg picture files. He explained that clicking on the images he retrieved allowed him to see the pathname for the image, tracing it to particular folders on the computer's hard drive. This process revealed folder and file names suggestive of child pornography. Kanatzar estimated it took five minutes to see depictions of child pornography. At that point, however, Cheatham came back into the room, told Kanatzar that Ray Andrus was on his way home, and asked Kanatzar to stop the search. Kanatzar testified he shut down his laptop computer.

The district court determined Dr. Andrus' consent was voluntary, but concluded Dr. Andrus lacked actual authority to consent to a computer search. The court based its actual authority ruling on its findings that Dr. Andrus did not know how to use the computer, had never used the computer, and did not know the user name that would have allowed him to access the computer.

The district court then proceeded to consider apparent authority. It indicated the resolution of the apparent authority claim in favor of the government was a "close call." The court concluded the agents' belief that Dr. Andrus had authority to consent to a search of the computer was reasonable up until the time they learned there was only one computer in the house. Because Cheatham instructed Kanatzar to suspend the search at that point, there was no Fourth Amendment violation.

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority

---

[23] [n.1] Kanatzar testified that someone without forensic equipment would need Ray Andrus' user name and password to access files stored within Andrus' user profile.

to consent to the search. When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object. The Supreme Court's most recent pronouncement on third party consent searches underscores that reasonableness calculations must be made in the context of social expectations about the particular item to be searched. The Court explained, "The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations." For example, the Court said, "[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent."

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." Password-protected files have been compared to a "locked footlocker inside the bedroom."

Because intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that "command[ ] a high degree of privacy."

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. Determining whether a computer is "locked," or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile." *See* Oxford English Dictionary Online, http://dictionary.oed.com (last visited Dec. 22, 2006) (entry for "Password," definition 1.b.: defining "password" in the computing context as "[a] sequence of characters, known only to authorized persons, which must be keyed in to gain access to a particular computer, network, file, function, etc."). The presence of a password that limits access to the computer's contents may only be discovered by starting up the machine or attempting to access particular files on the computer as a normal user would.[n.5][24]

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers' knowledge about password protection as an indication of whether a computer is "locked" in the way a footlocker would be. For example, in *Trulock* [*v. Freeh*, 275 F.3d 391 (4th Cir. 2001)], the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's

---

[24] [n.5] The difficulty with seeing a "lock" on computer data is exacerbated by the forensic software sometimes used by law enforcement to conduct computer searches. The software, like the EnCase software used by Agent Kanatzar, allows user profiles and password protection to be bypassed.

computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. The court in that case explained, "Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files." In *United States v. Morgan*, the Sixth Circuit viewed a wife's statement to police that she and her husband did not have individual usernames or passwords as a factor weighing in favor of the wife's apparent authority to consent to a search of the husband's computer. 435 F.3d 660, 663 (6th Cir. 2006). A critical issue in assessing a third party's apparent authority to consent to the search of a home computer, therefore, is whether law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password protected.

In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members' access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer's files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority.

First, the officers knew Dr. Andrus owned the house and lived there with family members. Second, the officers knew Dr. Andrus' house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus' room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search. It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus' computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer's password protection indicated his computer was "locked" to third parties, a fact the officers would have known had they asked questions of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. In essence, by suggesting the onus was on the officers to ask about password protection prior to searching the computer, Andrus necessarily submits there is inherent ambiguity whenever police want to search a household computer and a third party has not affirmatively provided information about his own use of

the computer or about password protection. Andrus' argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users. The dissent, however, is critical of this court because it neither makes the argument for Andrus nor supplies the evidence to support the argument. The key aspect of the dissent is its criticism of the majority for refusing to "take judicial notice that password protection is a standard feature of operating systems." A judicially noticed fact is "one not subject to reasonable dispute in that it is either (1) generally known . . . or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Fed.R.Evid. 201(b). Although judicial notice may be taken *sua sponte*, it would be particularly inappropriate for the court to wander undirected in search of evidence irrefutably establishing the facts necessary to support the dissent's conclusion regarding the absence of apparent authority: namely, that (a) password protection is a standard feature of most operating systems; (b) most users activate the standard password-protection feature; and (c) these are matters of such common knowledge that a reasonable officer would make further inquiry. Without a factual basis on which to proceed, we are unable to address the possibility that passwords create inherent ambiguities.[n.8][25]

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, *one* user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus' computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers' belief in Dr. Andrus' authority at the outset of the computer search.

McKAY, Circuit Judge, dissenting.

I take issue with the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party's access to that password.

The development of computer password technology no doubt "presents a challenge distinct from that associated with other types of" *locked* containers. The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether

---

[25] [n.8] If the factual basis were provided, law enforcement's use of forensic software like EnCase, which overrides any password protection without ever indicating whether such protection exists, may well be subject to question. This, however, is not that case.

such passwords have been enabled does not "exacerbate[ ]" this difficulty; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were "shown to be commonplace, law enforcement's use of forensic software like EnCase . . . may well be subject to question." But the fact that a computer password "lock" may not be *immediately* visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.[n.3][26]

The fact remains that EnCase's ability to bypass security measures is well known to law enforcement. Here, ICE's forensic computer specialist found Defendant's computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant's computer and ran the EnCase program. The agents made no effort to ascertain whether such security was enabled prior to initiating the search. The testimony makes clear that such protection was discovered during additional computer analysis conducted at the forensic specialist's office.

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus' status as a renter and Dr. Andrus' ability to enter his 51-year-old son's bedroom in order to determine Dr. Andrus' ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son's password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant's computer was the only one in the house, and they began to doubt Dr. Andrus' authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant's room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. The consent form, which Dr. Andrus signed prior to even showing the agents Defendant's computer, indicates that Dr. Andrus consented to the search of only a single "computer," rather than computers. In addition, the local police officer accompanying the ICE agents heard Dr. Andrus tell his wife that the agents wanted to search *Defendant's* computer, which would have caused a reasonable law enforcement official to question Dr. Andrus' ownership and use of the computer.

The record reflects that, even prior to the agent's arrival at the target home, the agents were cognizant of the ambiguity surrounding the search. The agents testified that they suspended their search due to doubts regarding Dr. Andrus' ability to consent only after they learned that the internet service used by Defendant came bundled with the cable television service and was paid by Dr. Andrus. The district court noted, however, that the agents were aware of this fact

---

[26] [n.3.] I recognize that the ability of users to program automatic log-ins and the capability of operating systems to "memorize" passwords poses potential problems, since these only create the appearance of a restriction without actually blocking access.

prior to the search, having subpoenaed the internet/cable records from the service provider prior to their "knock-and-talk." Given the inexcusable confusion in this case, the circumstantial evidence is simply not enough to justify the agents' use of EnCase software without making further inquiry.

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer.

UNITED STATES v. FRANK GARY BUCKNER

473 F.3d 551 (4th Cir. 2007)

Diana Gribbon Motz, Circuit Judge.

This criminal investigation began when the Grottoes, Virginia police department received a series of complaints regarding online fraud committed by someone using AOL and eBay accounts opened in the name Michelle Buckner. On July 28, 2003, police officers went to the Buckner residence to speak with Michelle, but only Frank Buckner was at home. The officers then left, asking Frank to have Michelle contact them. A short while later, Frank Buckner himself called the police, seeking more information about why they wanted to speak with Michelle. The police responded that they wanted to talk with her about some computer transactions. That evening, Michelle Buckner went to the police station and told officers that she knew nothing about any illegal eBay transactions, but that she did have a home computer leased in her name. She further stated that she only used the home computer occasionally to play solitaire.

The next day, July 29, police returned to the Buckner residence to speak further with Michelle about the online fraud. Frank Buckner was not present. Michelle again cooperated fully, telling the officers "to take whatever [they] needed" and that she "want[ed] to be as cooperative as she could be." The computer Michelle had indicated was leased in her name was located on a table in the living room, just inside the front door of the residence. Pursuant to Michelle's oral consent, the officers seized the leased home computer.

At the time the officers seized the computer, it was turned on and running, with the screen visibly lit. The officers did not, at this time, open any files or look at any information on the computer. Instead, with Michelle's blessing, they shut down the computer and took its data — storage components for later forensic analysis. This analysis consisted of "mirroring" — that is, creating a copy of — the hard drive and looking at the computer's files on the mirrored copy.

At a suppression hearing, Frank Buckner offered the only affirmative evidence on

the password issue, testifying that a password was required to use the computer. Buckner stated that he was the only person who could sign on to the computer and the only person who knew the password necessary to view files that he had created. Nothing in the record contradicts this testimony. Nor, however, is there any record evidence that the officers knew this information at the time they seized or searched the computer. Indeed, the evidence indicates that no officer, including the officer who conducted the search of the mirrored hard drive, ever found any indication of password protection. The Government's evidence was that its forensic analysis software would not necessarily detect user passwords.[n.1][27]

In *Trulock* [*v. Freeh*, 275 F.3d 391 (4th Cir. 2001)], we held that a co-resident of a home and co-user of a computer, who did not know the necessary password for her co-user's password-protected files, lacked the authority to consent to a warrantless search of those files. We likened these private files to a "locked box" within an area of common authority. Although common authority over a general area confers actual authority to consent to a search of that general area, it does not "automatically . . . extend to the interiors of every discrete enclosed space capable of search within the area."

The logic of *Trulock* applies equally here. "By using a password," Frank Buckner, like Trulock, "affirmatively intended to exclude . . . others from his personal files." For this reason, "it cannot be said that" Buckner "assumed the risk" that a joint user of the computer, not privy to password-protected files, "would permit others to search his files." Thus, Michelle Buckner did not have actual authority to consent to a search of her husband's password-protected files because she did not share "mutual use, general access or common authority" over those files.

Michelle's lack of actual authority, however, does not end our inquiry. Rather, it would be sufficient that Michelle had apparent authority to consent to the search at issue.

Frank Buckner contends that Michelle did not have common authority over his computer files — a fact that the officers must have known, according to Buckner, because Michelle had told them that she was not computer-savvy and that she only used the computer to play games.

Whether the officers reasonably believed that Michelle had authority to consent to a search of all the contents of the computer's hard drive, however, depends on viewing these facts in light of the *totality* of the circumstances known to the officers at the time of the search. At that time, the officers knew that the computer was located in a common living area of the Buckners' marital home, they observed that the computer was on and the screen lit despite the fact that Frank Buckner was not present, and they had been told that fraudulent activity had been conducted from that computer using accounts opened in *Michelle's* name. The officers also knew that the machine was leased solely in *Michelle's* name and that she had the ability to return the computer to the rental agency at any time, without Frank Buckner's knowledge or consent.

---

[27] [n.1] The parties agree that none of Frank Buckner's files were encrypted. Nor is there any contention that the police officers *deliberately* used software that would avoid discovery of any existing passwords.

Furthermore, the officers did not have any indication from Michelle, or any of the attendant circumstances, that any files were password-protected. Even during the mirroring and forensic analysis processes, nothing the officers saw indicated that any computer files were encrypted or password-protected.[n.3][28] Despite Michelle's suggestion that she lacked deep familiarity with the computer, the totality of the circumstances provided the officers with the basis for an objectively reasonable belief that Michelle had authority to consent to a search of the computer's hard drive. Therefore, the police were justified in relying on Michelle's consent to search the computer and all of its files, such that no search warrant was required.

NOTE

EnCase is a software tool made by Guidance Software that is used by many computer forensic examiners. *See* www.guidancesoftware.com. It is very configurable. Should courts construe the Fourth Amendment to require investigators to determine the existence of password protection prior to examining a digital device? In all situations or only when there is reason to suspect that the device is used by more than one person? If password protection is discovered, what may an investigator then be permitted to do?

§ 7.4 FIFTH AMENDMENT PRIVILEGE: REQUIRING THE DISCLOSURE OF PASSWORDS, DECRYPTED FILES

"Encryption involves the encoding of information, called 'plaintext,' into unreadable form, termed 'ciphertext.' The reverse process of transforming the ciphertext back into readable plaintext is called decryption. The purpose, of course, is to prevent anyone other than the user or intended recipient from reading private information."[29]

> Encryption has become pervasive in our modern, technologically oriented society. In the home, encryption technology can be found in a multitude of devices. DVD and Blu-ray players perform decryption of encrypted, copyrighted movies. Wireless routers utilize encryption for security over the air. Every time someone uses the Internet to pay bills or to make purchases online, that person uses encryption technology. Commercially, companies use encryption to protect their data and to allow employees to securely access company networks from home through a Virtual Private Network.

---

[28] [n.3] We do not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place by the user.

[29] John Duong, Note, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL L. REV. 313, 324 (2009). Copyright © 2009, Drexel Law Review. All rights reserved. Reprinted by permission.

> Devices, both hardware and software, that utilize various encryption schemes are commonplace. Popular operating systems for computers, such as Microsoft Windows and Mac OS X, have some form of built-in encryption function that makes it easier for the public to use encryption technology. Commercial software is readily available to perform encryption of data and email. In addition to software-only solutions, hardware manufacturers have even launched products that have built-in, automatic encryption, making it virtually transparent to the end user who need not understand the underlying encryption technology in order to use it. One thing is certain: encryption exists to protect information, whether commercial or private.
>
> Today's encryption algorithms utilize complex mathematical routines to make it virtually impossible, given the computing power available today and in the foreseeable future, to "brute force" a passphrase. Even assuming that the government has the necessary computer processing power, there is still the question of whether it is even feasible given the resources necessary to perform the process of decryption. Without even knowing what the encrypted contents hold, it may be prohibitively expensive in time and cost to attempt decryption.[30]

IN RE GRAND JURY SUBPOENA TO SEBASTIEN BOUCHER

2009 US. Dist. Lexis 13006 (D. Vt. 2009)

William K. Sessions, III, Chief Judge.

The Government appeals the United States Magistrate Judge's Opinion and Order granting defendant Sebastien Boucher's motion to quash a grand jury subpoena on the grounds that it violates his Fifth Amendment right against self-incrimination. The grand jury subpoena directs Boucher to

> provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

In its submission on appeal, the Government stated that it does not in fact seek the password for the encrypted hard drive, but requires Boucher to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury. The Government stated that it intends only to require Boucher to provide an unencrypted version of the drive to the grand jury.

On December 17, 2006, Boucher and his father crossed the Canadian border into the United States at Derby Line, Vermont. A Custom and Border Protection inspector directed Boucher's car into secondary inspection. The inspector conducting the secondary inspection observed a laptop computer in the back seat of Boucher's car,

---

[30] *Id.* at 324-28.

which Boucher acknowledged as his. The inspector searched the computer files and found approximately 40,000 images.

Based upon the file names, some of the files appeared to contain pornographic images, including child pornography. The inspector called in a Special Agent for Immigration and Customs Enforcement with experience and training in recognizing child pornography. The agent examined the computer and file names and observed several images of adult pornography and animated child pornography. He clicked on a file labeled "2yo getting raped during diaper change," but was unable to open it. The "Properties" feature indicated that the file had last been opened on December 11, 2006.

After giving Boucher *Miranda* warnings, and obtaining a waiver from him, the agent asked Boucher about the inaccessible file. Boucher replied that he downloads many pornographic files from online newsgroups onto a desktop computer and transfers them to his laptop. He stated that he sometimes unknowingly downloads images that contain child pornography, but deletes them when he realizes their contents.

The agent asked Boucher to show him the files he downloads. Boucher navigated to drive "Z" of the laptop, and the agent began searching the Z drive. The agent located and examined several videos or images that appeared to meet the definition of child pornography.

The agent arrested Boucher, seized the laptop and shut it down. He applied for and obtained a search warrant for the laptop. In the course of creating a mirror image of the contents of the laptop, however, the government discovered that it could not find or open the Z drive because it is protected by encryption algorithms from the computer software "Pretty Good Protection," which requires a password to obtain access. The government is not able to open the encrypted files without knowing the password. In order to gain access to the Z drive, the government is using an automated system which attempts to guess the password, a process that could take years.

The Fifth Amendment to the United States Constitution protects "a person . . . against being incriminated by his own compelled testimonial communications." *Fisher v. United States*, 425 U.S. 391, 409 (1976). There is no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy Fifth Amendment protection.

"Although the contents of a document may not be privileged, the act of producing the document may be." "'The act of production' itself may implicitly communicate 'statements of fact.' By 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.'" *United States v. Hubbell*, 530 U.S. 27, 36 (2000). Thus, "the Fifth Amendment applies to acts that imply assertions of fact." It is "the attempt to force [an accused] to 'disclose the contents of his own mind' that implicates the Self-Incrimination Clause." Moreover, "[c]ompelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory."

At issue is whether requiring Boucher to produce an unencrypted version of his

laptop's Z drive would constitute compelled testimonial communication. *See In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992 (*In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir.1993) ("Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled and, if not, whether the act of producing it would constitute compelled testimonial communication . . . regardless of 'the contents or nature of the thing demanded.'").

The act of producing documents in response to a subpoena may communicate incriminating facts "in two situations: (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents."

Where the existence and location of the documents are known to the government, "no constitutional rights are touched," because these matters are a "foregone conclusion." The Magistrate Judge determined that the foregone conclusion rationale did not apply, because the government has not viewed most of the files on the Z drive, and therefore does not know whether most of the files on the Z drive contain incriminating material. Second Circuit precedent, however, does not require that the government be aware of the incriminatory *contents* of the files; it requires the government to demonstrate "with reasonable particularity that it knows of the existence and location of subpoenaed documents."

Thus, where the government, in possession of a photocopy of a grand jury target's daily calendar, moved to compel compliance with a subpoena for the original, the Second Circuit ruled that no act of production privilege applied. The existence and location of the calendar were foregone conclusions, because the target had produced a copy of the calendar and testified about his possession and use of it.

The target's production of the original calendar was also not necessary to authenticate it; the government could authenticate the calendar by establishing the target's prior production of the copy and allowing the trier of fact to compare the two.

Boucher accessed the Z drive of his laptop at the ICE agent's request. The ICE agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography. The Government thus knows of the existence and location of the Z drive and its files. Again providing access to the unencrypted Z drive "adds little or nothing to the sum total of the Government's information" about the existence and location of files that may contain incriminating information.

Boucher's act of producing an unencrypted version of the Z drive likewise is not necessary to authenticate it. He has already admitted to possession of the computer, and provided the Government with access to the Z drive. The Government has submitted that it can link Boucher with the files on his computer without making use of his production of an unencrypted version of the Z drive, and that it will not use his act of production as evidence of authentication.

Because Boucher has no act of production privilege to refuse to provide the grand jury with an unencrypted version of the Z drive of his computer, his motion to quash the subpoena (as modified by the Government) is denied. Boucher is directed to

provide an unencrypted version of the Z drive viewed by the ICE agent. The Government may not make use of Boucher's act of production to authenticate the unencrypted Z drive or its contents either before the grand jury or a petit jury.

NOTES

1. Compare the views expressed in John Duong, Note, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL L. REV. 313, 349-50 (2009):

> Unlike physical evidence, which exists independently from the person, there is no such separation between a person and his or her passphrase. The passphrase is inherently intertwined within the chasms of the mind of the individual. In other words, being compelled to produce a passphrase involves mining and extracting the contents of one's mind and that act itself inherently involves revealing the contents of that mind, which makes it a testimonial communication. This link simply cannot be conceptually severed.

2. Duong, in his Note, also argues:

> [T]he District Court [in *Boucher*] erred . . . by claiming that the government already knew "of the existence and location of the Z drive and its files." This is precisely the kind of fishing expedition that the *Hubbell* Court rejected. In *Hubbell*, the Supreme Court stated that a broad-based belief of certain materials is not enough for application of the forgone conclusion doctrine. The government must be able to specify that it knew such materials existed and where they were located. In this case, the government only knew the existence and location of some of the child pornography files. Contrary to the District Court's assertion that the contents of the entire decrypted Z drive would not add much to the sum total of the government's knowledge, it could in fact add considerably if Boucher had many more incriminating files than were previously viewed by the Customs agents. The District Court should have performed the same analysis and held that Boucher must only produce the files of which the government already had prior knowledge.

Id. at 355 n.210.

3. **An Ethical quandary?** When faced with the order by the court in *Boucher*, as his attorney, what advice could you ethically provide? What are the consequences of refusing to comply with the court order vs. a possible conviction for child pornography charges?

4. The reasonableness of the search and seizure of computers at the International border is considered in Chapter 10.