COMPUTER CRIME LAW

Orin S. Kerr

2008 Supplement

This supplement was prepared for use with the First Edition of Kerr, Computer Crime Law (Thomson-West 2006). It is current through November 2007. This supplement can be downloaded as a free .pdf file at www.volokh.com/files/2008supplement.pdf. Permission is granted for copying and distributing this supplement for classroom or other scholarly use.

Orin S. Kerr
Washington DC.

Table of Contents

Chapter 2: Computer Misuse	2
United States v. Phillips	2
Chapter 3: Traditional Crimes	6
United States v. Corrar	6
United States v. Kuchinski	10
Chapter 5: The Fourth Amendment	13
United States v. Andrus	13
United States v. Forrester	24
Warshak v. United States	28
United States v. D'Andrea	39
Chapter 6: Statutory Protections	43
Chapter 7: Jurisdiction	45
United States v. Vilar	45
Chapter 8: National Security	51

CHAPTER 2:
COMPUTER MISUSE

On page 74, before the heading "Computer Fraud Statutes," add the following new case:

UNITED STATES v. PHILLIPS

United States Court of Appeals for the Fifth Circuit, 2007.
477 F.3d 215.

EDITH H. JONES, Chief Judge:

Christopher Andrew Phillips appeals his conviction for intentionally accessing a protected computer without authorization and recklessly causing damage in excess of $5,000, pursuant to the Computer Fraud and Abuse Act,18 U.S.C. §§ 1030(a)(5)(A)(ii) and (B)(i). Phillips alleges that (1) insufficient evidence was presented at trial to support his conviction under § 1030(a)(5)(A)(ii) . . . . Finding no reversible error, we affirm.

BACKGROUND

Phillips entered the University of Texas at Austin ("UT") in 2001 and was admitted to the Department of Computer Sciences in 2003. Like all incoming UT students, Phillips signed UT's "acceptable use" computer policy, in which he agreed not to perform port scans using his university computer account.[1] Nonetheless, only a few weeks after matriculating, Phillips began using various programs designed to scan computer networks and steal encrypted data and passwords. He succeeded in infiltrating hundreds of computers, including machines belonging to other UT students, private businesses, U.S. Government agencies, and the British Armed Services webserver. In a matter of months, Phillips amassed a veritable informational goldmine by stealing and cataloguing a wide variety of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers.

The scans, however, were soon discovered by UT's Information Security Office ("ISO"), which informed Phillips on three separate occasions that his computer had been detected portscanning hundreds of thousands of external computers for vulnerabilities. Despite several instructions to stop, Phillips continued to scan and infiltrate computers within and without the UT system, daily adding to his database of stolen information.

[1] Port scanning is a technique used by computer hackers by which an individual sends requests via a worm or other program to various networked computer ports in an effort to ascertain whether particular machines have vulnerabilities that would leave them susceptible to external intrusion. Often used as an initial step in launching an attack on another computer or transmitting a virus, port scanning is a relatively unsophisticated, but highly effective, reconnaissance method, likened at trial by UT's information technology chief as the electronic equivalent of "rattling doorknobs" to see if easy access can be gained to a room.

At around the time ISO issued its first warning in early 2002, Phillips designed a computer program expressly for the purpose of hacking into the UT system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was a "secure" server operated by UT and used by faculty and staff as a resource for enrollment in professional education courses. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Phillips exploited the vulnerability inherent in this log-on protocol by transmitting a "brute-force attack" program,[2] which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users.

Initially, Phillips selected ranges of Social Security numbers for individuals born in Texas, but he refined the brute-force attack to include only numbers assigned to the ten most populous Texas counties. When the program hit a valid Social Security number and obtained access to TXClass, it automatically extracted personal information corresponding to that number from the TXClass database and, in effect, provided Phillips a "back door" into UT's main server and unified database. Over a fourteen-month period, Phillips thus gained access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.

Phillips's actions hurt the UT computer system. The brute-force attack program proved so invasive -- increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000 -- that it caused the UT computer system to crash several times in early 2003. Hundreds of UT web applications became temporarily inaccessible, including the university's online library, payroll, accounting, admissions, and medical records. UT spent over $122,000 to assess the damage and $60,000 to notify victims that their personal information and Social Security numbers had been illicitly obtained.

After discovering the incursions, UT contacted the Secret Service, and the investigation led to Phillips. Phillips admitted that he designed the brute-force attack program to obtain data about individuals from the UT system, but he disavowed that he intended to use or sell the information.

Phillips was indicted and convicted after a jury trial on one count of computer fraud pursuant to 18 U.S.C. § 1030(a)(5)(A)(ii) and (B)(i), and one count of possession of an identification document containing stolen Social Security numbers pursuant to 18 U.S.C. § 1028(a)(6). Phillips timely filed a motion for judgment of acquittal [under Fed. R. Crim. P. 29] challenging, unsuccessfully, the sufficiency of the evidence regarding the loss amount used to support the computer fraud conviction. . . . He was sentenced to five years' probation, five hundred hours of community service, and restitution of $170,056. Phillips appealed.

DISCUSSION

Phillips asserts that the Government failed to produce sufficient evidence that he "intentionally access[ed] a protected computer without authorization" under § 1030(a)(5)(A)(ii).

---

[2] Brute-force attack" is term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords.

Although Phillips timely filed a motion for judgment of acquittal, see Fed.R.Crim.P. 29, the motion raised only the narrow issue whether the loss or damage caused by his online exploits exceeded $5,000.00. See § 1030(a)(5)(B)(i). Both the Government's opposition memorandum and the district court's ruling on the motion addressed this one issue. Accordingly, where, as here, a defendant asserts specific grounds for a specific element of a specific count for a Rule 29 motion, he waives all others for that specific count. We thus review his newly raised claim that there was insufficient evidence of the statutorily required mens rea under § 1030(a)(5)(A)(ii) only for a "manifest miscarriage of justice." United States v. Green, 293 F.3d 886, 895 (5th Cir.2002) Under this exacting standard of review, a claim of evidentiary insufficiency will be rejected unless the record is devoid of evidence pointing to guilt or if the evidence is so tenuous that a conviction is shocking.

Phillips's insufficiency argument takes two parts: that the Government failed to prove (1) he gained access to the TXClass website without authorization and (2) he did so intentionally.

With regard to his authorization, the CFAA does not define the term, but it does clearly differentiate between unauthorized users and those who "exceed[ ] authorized access." Several subsections of the CFAA apply exclusively to users who lack access authorization altogether. See, e.g., §§ 1030(a)(3), (5)(A)(i), (5)(A)(ii), (5)(A)(iii). In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between "insiders, who are authorized to access a computer," and "outside hackers who break into a computer." See S.Rep. No. 104-357, at 11 (1996).

Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user. Applying such an intended-use analysis, in United States v. Morris, 928 F.2d 504 (2d Cir.1991), a case involving an invasive procedure that prefigured modern portscanning, the Second Circuit held that transmission of an internet worm designed "to demonstrate the inadequacies of current security measures on computer networks by exploiting ... security defects" was sufficient to permit a jury to find unauthorized access within the meaning of § 1030(a)(5)(A). The Morris court determined that conduct, like "password guessing" or finding "holes in ... programs," that uses computer systems not "in any way related to their intended function" amounts to obtaining unauthorized access. Id. at 510; see also Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir.2004) (internet site administrator's misappropriation of login names and passwords to obtain access to competitor's website violated CFAA); Theofel v. Farey-Jones, 359 F.3d 1066, 1074 (9th Cir. 2004) (use of an authorized third-party's password by an outside hacker to gain access to a mail server fell within "the paradigm of what [Congress] sought to prohibit [under the Stored Communications Act]"); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n. 10 (1st Cir.2001) (mentioning in dicta the district court's observation of a "default rule" that conduct is unauthorized for § 1030 purposes "if it is not in line with reasonable expectations of the website owner and its users").

Phillips's brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data that he was not permitted to view or

use. During cross-examination, Phillips admitted that TXClass's normal hourly hit volume did not exceed a few hundred requests, but that his brute-force attack created as many as 40,000. He also monitored the UT system during the multiple crashes his program caused, and backed up the numerical ranges of the Social Security numbers after the crashes so as not to omit any potential matches. Phillips intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data. There was no lack of evidence to find him guilty of intentional unauthorized access.

Phillips makes a subsidiary argument that because the TXClass website was a public application, he, like any internet user, was a de facto authorized user. In essence, Phillips contends that his theft of other people's data from TXClass merely exceeded the preexisting generic authorization that he maintained as a user of the World Wide Web, and he cannot be considered an unauthorized user under § 1030(a)(5)(A)(ii).

This argument misconstrues the nature of obtaining "access" to an internet application and the CFAA's use of the term "authorization." While it is true that any internet user can insert the appropriate URL into a web browser and thereby view the "TXClass Administrative Training System" log-in web page, a user cannot gain access to the TXClass application itself without a valid Social Security number password to which UT has affirmatively granted authorization.[3] Neither Phillips, nor members of the public, obtain such authorization from UT merely by viewing a log-in page, or clicking a hypertext link. Instead, courts have recognized that authorized access typically arises only out of a contractual or agency relationship.[4] While Phillips was authorized to use his UT email account and engage in other activities defined by UT's acceptable computer use policy, he was never authorized to access TXClass. The method of access he used makes this fact even more plain. In short, the government produced sufficient evidence at trial to support Phillips's conviction under § 1030(a)(5)(A)(ii).

CONCLUSION

For the foregoing reasons, the conviction and sentence are affirmed.

---

[3] Phillips's contention that an individual's ability to view TXClass's log-in webpage amounts to a general grant of authorized access to the public-at-large is unsupported by various judicial interpretations of what constitutes obtaining access to a protected computer. See, e.g., State v. Allen, 260 Kan. 107, 917 P.2d 848 (1996) (under Kansas computer crime statute, until a computer user proceeds beyond introductory banners and log-in screens by use of a password, he has not accessed the program); State v. Riley, 121 Wash.2d 22, 846 P.2d 1365 (1993) (en banc) (attempted entry into computer using randomly generated passwords is not access until a successful password is found allowing entry); see also Role Models, Inc. v. Jones, 305 F.Supp.2d 564 (D.Md.2004) (mere receipt of information from a protected computer is not equivalent to obtaining access under CFAA).

[4] See, e.g., Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir.2006) (authorized access to company computer terminated when employee violated employment contract); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir.2001) (confidentiality agreement defined authorized access to travel company's computerized pricing information); United States v. Czubinski, 106 F.3d 1069 (1st Cir.1997) (employer assignment of a confidential password created authorization); Shurgard Storage Ctrs., Inc. v. Safeguard Self-Storage, Inc., 119 F.Supp.2d 1121 (W.D.Wash.2000) (employees not authorized to obtain proprietary information from former employer because agency relationship had terminated).

CHAPTER 3:
TRADITIONAL CRIMES

On page 191, immediately after United States v. Cohen, add the following new case:

UNITED STATES v. CORRAR

United States District Court for the Northern District of Georgia, 2007.
--- F.Supp.2d ----, 2007 WL 196862

JULIE E. CARNES, District Judge.

This is a case about an attempt to collect on a gambling debt. The United States alleges that Danny Corrar ("Defendant"), Patricia Affatigato, and Mikey Glorioso are "agents" for PlayWithAl.com ("PWA"), an online sports book operating out of the Netherlands, Antilles. All three, the Government asserts, were involved in an effort to collect a debt from Larry Parker, a Georgia resident, and himself an agent of PWA. Affatigato was not before the Court at trial. Meanwhile, this Court entered a judgment of acquittal on the only count with which Glorioso was charged, thereby dismissing him from the case. The remaining charges against defendant, however, went before a jury, which convicted him of violating . . . the Wire Act, 18 U.S.C. § 1084.

[The prosecution stems] from defendant's efforts to collect an outstanding debt from Parker. Parker is a bar manager who first began betting with PWA when he lived in Florida. In June of 2002, Parker moved to Georgia, where his former contact with PWA put him in touch with defendant, a resident of New York, who, together with Affatigato, operate a children's entertainment business. Defendant set Parker up as an "agent" of PWA, providing him with ten account numbers which he could distribute to his friends and customers. This scheme did not require Parker to personally receive or transmit his friends' wagers. Parker testifies that he was initially reluctant to hand out account numbers to his friends. This reluctance was apparently justified, because his friends lost money, and by the summer of 2002, Parker found himself on the hook to PWA for at least $20,000.

In response to his debt problems, Parker turned to the FBI, who helped him engage in wiretapping of his phone conversations with defendant and Affatigato. Parker contends that he never attempted to collect money from his friends to pay back his debt to PWA. In November of 2002, defendant visited Parker at his workplace, where Parker says defendant tried to collect the debt and became agitated and angry. In June of 2003, defendant again visited Georgia, this time accompanied by Glorioso, planning to meet Parker and to collect the debt. The meeting, however, was a sting, and both defendant and Glorioso were arrested.

Count Three of the indictment alleges a violation of the Wire Act. The Wire Act, codified at 18 U.S.C. § 1084, provides that:

> Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest ... shall be fined under this title or imprisoned not more than two years, or both.

Defendant asserts that the Wire Act does not reach his conduct for two reasons. First, he contends that he was not "engaged in the business of betting or wagering." Second, he contends that the information he provided Parker did not "assist[ ] in the placing of bets or wagers." Neither of these arguments is persuasive.

A. Engaged in the Business of Betting or Wagering

Defendant's contention that he was not "engaged in the business of betting or wagering" is based on the observation that Wire Act prosecutions "have historically been limited to persons involved in actual bookmaking activities." Even if this characterization of the history of Wire Act prosecutions were correct, it would not prevent the United States from prosecuting other defendants who did not engage in bookmaking, but whose acts are prohibited by the statute. That the United States has often used the Wire Act to prosecute bookmakers does not estop the Government from bringing charges against other persons whose conduct the Act criminalizes. Neither the text of the Wire Act nor the case law interpreting it requires the narrow reading that the defendant suggests. If Congress sought only to criminalize bookmaking, "being engaged in the business of betting or wagering" would simply read "receives bets or wagers." Each business is not comprised of a single job. Complex operations involve division of labor. Insisting that "the business of betting and wagering" is conducted solely by those individuals who actually accept bets is like saying that "the business of movie making" is conducted solely by camera men. Yet, actors, directors, and producers clearly have important roles in the film industry.

United States v. Cohen, 260 F.3d 68 (2nd Cir.2001), the most famous internet gambling case to date, so concludes. In *Cohen*, the Second Circuit affirmed the conviction on Wire Act charges of the founder and President of the World Sports Exchange, a successful online sports book based in Antigua. Defendant contends that this case is inapplicable, because Cohen was "running the show," whereas defendant is, at most, a middle man. Clearly, Cohen was not a "bookie" in the sense that defendant has used the term, because he did not personally accept bets or wagers from his customers. Within two years of founding his company, World Sports Exchange was receiving over 60,000 calls per month. Obviously, Cohen could not have handled this call volume himself. Instead, Cohen was a manager and promoter of his business, farming out the actual receipt of bets to others. The evidence at defendant's trial was sufficient to conclude that he engaged in similar management and promotion activities, albeit on a much lower scale that did not approach the level of success enjoyed by Cohen.

Defendant's attempt to reconcile *Cohen* with cases permitting the prosecution of individual bookies is unpersuasive. Under defendant's theory, both individual telephone operators who accept bets over the phone and the person "running the show" are subject to criminal sanction, but anyone who falls in between these two points is entirely off the hook. (Def. Br. at 12). Investors, managers, promoters, and agents are not liable under

defendant's theory, even if they did far more to spread the flow of illegal gambling than did individual telephone operators. This restriction does not flow from the text of the Wire Act, nor is it necessary. In this case, the Court instructed the jury that for defendant to be engaged in the business of betting, he must have "engaged in a regular course of conduct or series of transactions involving time, attention and labor devoted to betting or wagering for profit, rather than casual, isolated or sporadic transactions." That instruction serves to protect a defendant whose connection to the business of gambling is either attenuated or occasional.

B. Information Assisting in the Placing of Bets or Wagers

As noted, the Wire Act requires, as elements of the offense, that one be engaged in the business of betting or wagering and use a wire communication facility (telephone) for the transmission "of bets or wagers or information assisting in the placing of bets or wagers ..." Id. at 12 (emphasis added). Defendant argues that the information he provided to Parker did not assist Parker in placing bets.

As noted, utilizing a telephone, defendant provided Parker with account numbers that allowed him to place bets with PWA. Admittedly, in proving that a defendant provided "information assisting in the placing of bets," most prosecutions under this statute likely reference the information typically offered by bookies, such as the odds on a particular sporting event. The Court cannot say, however, that a defendant who provides the account numbers that make a bettor's subsequent wager possible has not provided "information". Certainly, these account numbers are not only helpful, but are required to place a bet with PWA. That Parker might have been able to gamble by other means or already had account numbers does not render this information useless. Therefore, defendant's Motion for a Judgment of Acquittal on Count Three of the indictment is hereby DENIED.

Defendant's more general argument that many people are unsure whether internet gambling is illegal does not change this analysis. Admittedly, there is some practical resonance to defendant's argument that it might not be obvious to the average person, on first blush, that defendant's conduct violated federal law. As the Government conceded, there is a dearth of cases in which defendants have been convicted under the Wire Act as a result of internet gambling, notwithstanding the fact that internet gambling appears to be quite widespread in this country. At trial, *Cohen* was the only case to which either party could cite. Moreover, as mentioned during trial, there was, at that time, a bill pending in the United States Senate to make payment for internet gambling illegal. (Def. Br. at 15 n. 3.) Although not dispositive, it appears that some members of Congress are likewise uncertain that existing law adequately proscribes internet gambling. Indeed, during the trial, this Court questioned the prudence of the prosecution, given the arguable uncertainty of the law, the de minimis scope of the defendant's activities, and the less than laudatory conduct and demeanor of the "victim" of the crime, Mr. Parker.

Notwithstanding the above observations, the Court concludes that defendant's conduct cannot be absolved through application of the "rule of lenity." First, as noted, there is at least one published case that has held that internet gambling operations can run afoul of the law: specifically, United States v. Cohen, 260 F.3d 68 (2nd Cir.2001). . . . Moreover, even if internet gambling were permissible under state law, using interstate wire communication facilities to promote it would not be. This is why the Wire Act,

unlike the Travel Act and 18 U.S.C. § 1955, does not require an underlying violation of state law. As this circuit has explained, "assistance to the states directly was only part of the reason for enactment of section 1084. This section was part of an omnibus crime bill that recognized the need for independent federal action to combat interstate gambling operations ... this series of legislation does not stand alone, but appears as part of an independent federal policy aimed at those who would, in furtherance of any gambling activity, employ any means within direct federal control." Martin v. United States, 389 F.2d 895, 898 (5th Cir.1968).

In short, for the above reasons, the Court DENIES defendant's Motion for a Judgment of Acquittal based on the Rule of Lenity.

On page 193, after note 3, add the following note:

4. In October 2006, Congress passed the Unlawful Internet Gambling Enforcement Act (UIGEA) as part of legislation tucked into an important law on safeguarding ports from terrorist attacks, the SAFE PORT Act. Pub. L. 109-347, Title VIII (codified as 31 U.S.C. §§ 5361, et seq.). The UIGEA regulates banks and credit card companies by prohibiting such companies from processing illegal bets. The basic idea is that banks and credit card companies will not do businesses with Internet gambling sites, and that some United States-based users of Internet gambling sites will be sufficiently discouraged by the difficulty of placing bets that they will place fewer bets or even none at all. For an introduction to the Act, see James N. Brenner, Note, *Betting On Success: Can The Unlawful Internet Gambling Enforcement Act Help The United States Achieve Its Internet Gambling Policy Goals?,* 30 Hastings Comm. & Ent L.J. 109 (2007).

On pages 224-29, replace United States v. Tucker with the following case:

UNITED STATES v. KUCHINSKI

United States Court of Appeals for the Ninth Circuit, 2006.
469 F.3d 853.

FERNANDEZ, Circuit Judge:

After obtaining information that Kuchinski was involved in child pornography, the FBI obtained a search warrant for his computer. Upon execution of that warrant, between 15,120 and 19,000 separate images of child pornography were recovered therefrom. Sixteen of those images were located in the computer's downloaded files and 94 were located in its deleted files (recycle bin). Kuchinski does not argue that he is not responsible for the possession of those images. However, 1,106 images were in the Active Temporary Internet Files and another 13,904 to 17,784 images were in the Deleted Temporary Internet Files. (These are sometimes hereafter referred to as the cache files.) Thereafter, Kuchinski was indicted for receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) (count I), possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B) (count II), and forfeiture of his computer equipment, 18 U.S.C. § 2253 (count III).

We have made it plain that a person does knowingly receive and possess child pornography images when he seeks them out over the internet and then downloads them to his computer. In fact, we have declared that, "[i]n the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it." *United States v. Romm*, 455 F.3d at 990 (9th Cir. 2006); *See also United States v. Tucker*, 305 F.3d 1193, 1204 (10th Cir.2002). Thus, Kuchinski properly concedes that he did knowingly receive and possess the 110 images that he downloaded. But he was charged with many more -- an additional 13,904 to 17,984 images, which appeared in his cache files. Did Kuchinski knowingly receive and possess the images in those files, or, rather, does the evidence support a determination that he did? We think not.

According to the evidence before the district court, when a person accesses a web page, his web browser will automatically download that page into his Active Temporary Internet Files, so that when the site is revisited the information will come up much more quickly than it would have if it had not been stored on the computer's own hard drive. When the Active Temporary Internet Files get too full, they spill excess saved information into the Deleted Temporary Internet Files. All of this goes on without any action (or even knowledge) of the computer user. A sophisticated user might know all of that, and might even access the files. But, "most sophisticated--or unsophisticated users don't even know they're on their computer."

Much of the above also appears in our discussion of this area in *United States v. Romm*. There we also pointed out that "the cache is a 'system-protected' area, which the operating system tries to prevent users from accessing by displaying a warning that access involves an 'unsafe' system-command." We also noted that a user, who knows what he is doing, can go forward and get access to the cache files anyway. In the case at

hand, there was no evidence that Kuchinski was sophisticated, that he tried to get access to the cache files, or that he even knew of the existence of the cache files.

There is no question that the child pornography images were found on the computer's hard drive and that Kuchinski possessed the computer itself. Also, there is no doubt that he had accessed the web page that had those images somewhere upon it, whether he actually saw the images or not. What is in question is whether it makes a difference that, as far as this record shows, Kuchinski had no knowledge of the images that were simply in the cache files. It does.

While we have not confronted this precise issue, we have come quite close. In *Romm*, 455 F.3d at 995-96, the evidence demonstrated that the defendant knew about the cache files and had actually taken steps to access and delete them. On appeal, he conceded knowledge, and contested dominion and control, but we rejected his arguments. In so doing, we opined that "to possess the images in the cache, the defendant must, at a minimum, know that the unlawful images are stored on a disk or other tangible material in his possession." *Id.* at 1000. We relied upon a case wherein the Tenth Circuit Court of Appeals had declared that the defendant was properly found guilty where he knew that child pornography images would be sent to his "browser cache file and thus saved on his hard drive." *Tucker*, 305 F.3d at 1204. As the court put it: "Tucker, however, intentionally sought out and viewed child pornography knowing that the images would be saved on his computer. Tucker may have wished that his Web browser did not automatically cache viewed images on his computer's hard drive, but he concedes he knew the web browser was doing so."

We were also at some pains to distinguish Romm's situation from one where it could be argued that "the cache is an area of memory and disk space available to the browser software, not to the computer user." *United States v. Gourde*, 440 F.3d 1065, 1082 (9th Cir.2006) (en banc) (Kleinfeld, J., dissenting). In *Romm*, we noted that we were confronting a different situation because Romm did have both knowledge of and access to his cache files.

Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control. Therefore, on this record it was not proper to consider the cache file images when Kuchinski's [criminal liability] was calculated. As a result, . . . we must vacate the sentence and remand.

On page 240, after note 4, add the following note:

5. *First Amendment Defenses to Mere Possession Charges?* On October 20, 2007, the U.S. Supreme Court held oral argument in *United States v. Williams*, a First Amendment challenge to 18 U.S.C. § 2252A(a)(3)(B). Section 18 U.S.C. § 2252A(a)(3)(B) is the so-called "pandering" statute; it prohibits presenting, promoting, or

advertising materials in a way that leaves the impression that they are images of child pornography.

During the oral argument, several Justices and the Solicitor General appeared to agree that there may be as-applied First Amendment defenses to charges for mere possession of child pornography beyond those in the narrow statutory "safety valve" exception. The issue arose in the context of understanding the relationship between possession offenses and pandering offenses. Consider the following exchange between the Justices and Solicitor General Paul Clement:

> JUSTICE KENNEDY: There are some terrible practices in the child-trafficking area where children are held in brothels for the most debased of acts. There are abuses in prisons, abuses in schools. If there are videotapes showing those things, it seems to me that the statute is -- that they're clearly covered by the statute, and maybe even a killing of a little girl in public might be sadistic. Assume that that's covered by the statute. Is there anything in the "presents" and the "promotes" language in the scienter component of the statute that gives some protection to these materials? Is it just [something raised in an] as-applied [constitutional challenge]? Is that what we have to do?
> GENERAL CLEMENT: Here is how I would try to analyze it, Justice Kennedy, which is I would say that there would be an as-applied challenge there because the basic prohibition on child pornography that would apply to the underlying materials, there would be an as-applied exception to that.
> JUSTICE KENNEDY: So we want the public to see this to show them how bad it is, and that is permitted under the statute, because it is not "presenting"?
> GENERAL CLEMENT: I mean there would be another way to try to get at that. . . . Because it would be clear that, although I was presenting it as visual depictions of children who had that happen to them, I was presenting it exclusively for its scientific, artistic, literary value.
> JUSTICE SCALIA: Of course, you have a problem not just with the presenting, not just with the pandering of it. You have a problem with the mere possession of it. You have to find some exception for that anyway. You have to find some as-applied challenge exception for the mere possession of it, even if you don't pander it.
> GENERAL CLEMENT: Well, Justice Scalia, that's exactly right. And that's why I would think the logical way to proceed would be you would find an as-applied exception to the basic prohibition. And then, naturally, that would apply to the pandering provision.

http://www.supremecourtus.gov/oral_arguments/argument_transcripts/06-694.pdf

How broad should the as-applied exception to liability for possession be? During the *Williams* argument, Justice Souter suggested that it may apply to cases of accidental possession; Justice Stevens suggested that it may apply when the image is of a person 17 years old. What should the test be?

CHAPTER 5:
THE FOURTH AMENDMENT

On page 335, at the end of note 5, add the following new case:

UNITED STATES v. ANDRUS

United States Court of Appeals for the Tenth Circuit, 2007.
483 F.3d 711.

MURPHY, Circuit Judge.

Defendant-Appellant Ray Andrus was indicted on one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Agents of the Bureau of Immigration and Customs Enforcement ("ICE") found pornographic images of children on Andrus' home computer after Andrus' father, Dr. Bailey Andrus, consented to a search of the Andrus home and Andrus' computer. Andrus moved to suppress the inculpatory evidence found on his computer during the search, arguing Dr. Andrus' consent was not voluntary and that Dr. Andrus lacked both actual and apparent authority to consent to a search of the computer. The district court determined Dr. Andrus' consent was voluntary and that Dr. Andrus had apparent authority to consent to the search. The district court, accordingly, denied Andrus' motion to suppress.

After the district court's denial of his motion, Andrus pleaded guilty to the charge against him but retained the right to appeal the district court's denial of his suppression motion. He was sentenced to seventy months' imprisonment followed by three years' supervised release. In this appeal, Andrus challenges the district court's denial of his suppression motion. Exercising jurisdiction under 28 U.S.C. § 1291, this court concludes Dr. Andrus had apparent authority to consent to a search of Ray Andrus' computer. We therefore affirm the district court's denial of Andrus' motion to suppress.

BACKGROUND

The federal investigation into the Andrus household began in January 2004 and focused primarily on Ray Andrus. At least one agent conducted surveillance on the Andrus residence and knew Ray Andrus worked at the Shawnee Mission School. 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 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.[5]

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 and waited in Ray Andrus' bedroom with the computer until Cheatham came back into the room to tell him Andrus had personally consented to the search and Kanatzar could continue.

Cheatham testified he asked Kanatzar to stop the computer search because of information revealed through his continuing conversation with Dr. Andrus. Cheatham explained he asked Dr. Andrus if there were other computers in the house and Dr. Andrus replied the computer in Ray Andrus' room was the only one. Cheatham then asked Dr. Andrus about the internet service and Dr. Andrus indicated it was part of the cable package. At that point, Ray Andrus was telephoned at his workplace. There is conflicting evidence concerning whether Dr. Andrus or Cheatham suggested calling Andrus. Dr. Andrus dialed Andrus' work number, spoke briefly with his son, and handed the phone to Cheatham.[6] At the conclusion of his conversation with Cheatham, Ray Andrus agreed to

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

[6] It is disputed whether Cheatham told Andrus during this phone call that child pornography had been found on his computer. Cheatham maintained he did not mention to Andrus that the computer search was already underway, while Andrus testified Cheatham told him during the phone call that pornography had been discovered during a search of his computer. Because of the conclusion that Dr. Andrus had apparent authority to consent to a search of the computer, we need not analyze the voluntariness of Ray

return to the Andrus residence. He arrived ten to twenty minutes later. He parked his car in the garage and was met by Cheatham, Woollen, and ICE Agent Smith, who arrived on the scene after the agents' initial entry into the Andrus residence. Cheatham testified he told Andrus that officers had already been inside the residence and had looked through his room. Cheatham's written report also indicates he told Andrus he had a computer technician at the residence and that Dr. Andrus had consented to a search of the house and the computer in Andrus' bedroom. Cheatham said he then verbally asked Andrus for consent to search his room and his computer. After obtaining Andrus' consent, Cheatham went back inside to authorize Kanatzar to continue his search.

Ray Andrus was indicted on one count of knowingly and intentionally possessing pornographic images of minors in violation of 18 U.S.C. § 2252(a)(4)(B). Claiming a Fourth Amendment violation, Andrus moved to suppress the evidence gathered from his residence and his computer. In the memorandum supporting his motion to suppress, Andrus argued: (1) Dr. Andrus' consent was not voluntary; (2) Dr. Andrus lacked actual authority to consent to a search of the computer, even if he had authority to consent to a search of Ray Andrus' room; and (3) Dr. Andrus could not reasonably be seen as having authority to consent to a search of the computer and, thus, lacked apparent authority.

The district court held an evidentiary hearing at which Detective Woollen, Agent Cheatham, Agent Kanatzar, Agent Smith, Dr. Andrus, and Ray Andrus testified. At the conclusion of the hearing, the 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. The court based its conclusion that Dr. Andrus had apparent authority on the following factual findings: (1) the email address bandrus@ kc. rr. com, an address associated with Dr. Bailey Andrus, was used to register with Regpay and procure child pornography; (2) Dr. Andrus told the agents he paid the household's internet access bill; (3) the agents knew several individuals lived in the household; (4) Ray Andrus' bedroom door was not locked, leading a reasonable officer to believe other members of the household could have had access to it; and (5) the computer itself was in plain view of anyone who entered the room and it appeared available for anyone's use. Implicit in the district court's analysis was the assumption that the officers could reasonably have believed Dr. Andrus accessed the internet through the computer in Ray Andrus' bedroom, thereby giving Dr. Andrus the authority to consent to a search of the computer.

Lastly, the court concluded Ray Andrus' later consent to search his computer and his admissions regarding additional evidence were knowing and voluntary. It found the agents had explained they were investigating violations of federal law regarding child

---

Andrus' subsequent consent and, therefore, need not address the district court's resolution of this factual dispute.

pornography, advised Andrus of the circumstances facing him, and told him he was not under arrest and was free to go at any time. The court further found that Andrus told the agents he wanted to clear up the matter and gave consent to search his computer. Based on these factual findings, the court concluded Andrus' consent was given knowingly and voluntarily. The district court denied Andrus' motion to suppress.

On appeal, Andrus contests the district court's apparent authority ruling. He contends that ambiguities in the situation facing the officers at the Andrus residence required the officers to ask further questions concerning Dr. Andrus' authority to consent to a computer search prior to commencing the search. Andrus also argues on appeal that his own consent, given after the allegedly illegal computer search yielded inculpatory evidence, did not cure the alleged illegality because the earlier search and his later consent were not sufficiently attenuated.

DISCUSSION

Subject to limited exceptions, the Fourth Amendment prohibits warrantless searches of an individual's home or possessions. Illinois v. Rodriguez, 497 U.S. 177, 181, (1990). Voluntary consent to a police search, given by the individual under investigation or by a third party with authority over the subject property, is a well-established exception to the warrant requirement. Valid third party consent can arise either through the third party's actual authority or the third party's apparent authority. A third party has actual authority to consent to a search if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes. Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses authority to consent. *See* Georgia v. Randolph, 547 U.S. 103 (2006).

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 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. In *Randolph*, 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." Id. at 1522.

Objects typically associated with high expectations of privacy include "mankind's valises, suitcases, footlockers, and strong boxes." United States v. Block, 590 F.2d 535, 541 (4th Cir.1978). It may be unreasonable for law enforcement to believe a third party has authority to consent to the search of an object typically associated with a high expectation of privacy, especially when the officers know or should know the owner has indicated the intent to exclude the third party from using or exerting control over the object.

This court has not previously considered expectations of privacy associated with a home computer in a third party consent situation. Tenth Circuit precedent thus far has dealt only with computer searches where police have a warrant or other justification for searching the computer, or when the defendant computer owner himself has consented to the search. Other courts have, however, analyzed third party authority to consent to the search of a home computer, focusing on the application of Fourth Amendment principles in this special case where it is unclear from a visual inspection of the outside of the computer whether the computer's owner has manifested a subjective expectation of privacy in the computer or its data.

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." United States v. Aaron, 33 Fed.Appx. 180, 184 (6th Cir.2006) (unpublished). Password-protected files have been compared to a "locked footlocker inside the bedroom." Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir.2001).

Given the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall. A personal computer is often a repository for private information the computer's owner does not intend to share with others.

> [F]or most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests-including perfect strangers-are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation.

United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir.2006) (en banc) (Kleinfeld, J., dissenting). See generally Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) ("Computers are playing an ever greater role in daily life and are recording a growing proportion of it. They are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more. Each new software application means another aspect of our lives monitored and recorded by our computers."). 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.[7]

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*, the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's 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. 275 F.3d at 398, 403. 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. See United States v. Buckner, 473 F.3d 551, 555-56 (4th Cir.2007) (determining wife's consent was valid where wife leased computer in her name, wife occasionally used computer, computer was found in living room, and fraudulent activity had been conducted from that computer using accounts opened in wife's name). 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. *Trulock*, 275 F.3d at 403.

Andrus' case presents facts that differ somewhat from those in other cases. Andrus' computer was located in a bedroom occupied by the homeowner's fifty-one year old son rather than in a true common area. Dr. Andrus, however, had unlimited access to the room. Law enforcement officers did not ask specific questions about Dr. Andrus' use of the computer, but Dr. Andrus said nothing indicating the need for such questions. The resolution of this appeal turns on whether the officers' belief in Dr. Andrus' authority

[7] 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. See, e.g., United States v. Buckner, 473 F.3d 551, 553 (4th Cir.2007) (stating government's evidence was that forensic software "would not necessarily detect user passwords" on password-protected computer files).

was reasonable, despite the lack of any affirmative assertion by Dr. Andrus that he used the computer and despite the existence of a user profile indicating Ray Andrus' intent to exclude other household members from using the computer.[8] For the reasons articulated below, this court concludes the officers' belief in Dr. Andrus' authority was reasonable.

The critical issue in our analysis is whether, under the totality of the circumstances known to Cheatham, Woollen, and Kanatzar, these officers could reasonably have believed Dr. Andrus had authority to consent to a search of the computer. Phrased in the negative, we must ask "whether the surrounding circumstances could conceivably be such that a reasonable person would doubt [Dr. Andrus' consent] and not act upon it without further inquiry." *Rodriguez*, 497 U.S. at 188. If the circumstances reasonably indicated Dr. Andrus had mutual use of or control over the computer, the officers were under no obligation to ask clarifying questions, even if, as the dissent notes, the burden would have been minimal in this particular case.

This court must accept the factual findings of the district court unless those findings are clearly erroneous. . . . 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, despite the absence of any indication that Dr. Andrus' access to the computer was limited by a password, 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." Although judicial notice may be taken sua sponte, Fed.R.Evid. 201(c), 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

[8] Although the district court did not make any factual findings as to whether the computer was password protected, there is evidence in the record suggesting the presence of a password. Determining whether a password was actually in place, however, is unnecessary for analyzing Dr. Andrus' apparent authority, since the password would not have been obvious to the officers at the time they obtained consent and commenced the search.

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. In rejecting this challenge, the court notes the dissent itself did not take up the search for facts that would meet the requirements of Rule 201(b). Without a factual basis on which to proceed, we are unable to address the possibility that passwords create inherent ambiguities.[9]

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.

This case concerns the reasonable expectation of privacy associated with password-protected computers. In examining the contours of a third party's apparent authority to consent to the search of a home computer, the majority correctly indicates that the extent to which law enforcement knows or should reasonably suspect that password protection is enabled is critical. We differ, however, over the extent to which the burden of inquiry should rest with law enforcement personnel. More specifically, 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.

Given the majority's correct decision to categorize computers as containers, with all the attendant protections afforded under the case law, whether a computer search is objectively reasonable depends upon fact-specific determinations in individual cases with no bright-line rules. The few cases confronting this issue pay particular attention to the presence or absence of password protection.

The presence of security on Defendant's computer is undisputed. Yet, the majority curiously argues that Defendant's use of password protection is inconsequential because Defendant failed to argue that computer password protection is "commonplace." Of course, the decision provides no guidance on what would constitute sufficient proof of the prevalence of password protection, nor does it explain why the court could not take judicial notice that password protection is a standard feature of operating systems. Despite recognizing the "pervasiveness of computers in American homes," and the fact that the "personal computer is often a repository for private information the computer's owner does not intend to share with others," the majority requires the invocation of

[9] 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.

magical language in order to give effect to Defendant's subjective intent to exclude others from accessing the computer.

The development of computer password technology no doubt "presents a challenge distinct from that associated with other types of" locked containers. But this difficulty does not and cannot negate Fourth Amendment protection to computer storage nor render an expectation of computer privacy unreasonable. The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether 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.[10]

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 majority points out that law enforcement "did not ask specific questions" about Dr. Andrus' use of the computer or knowledge of Ray Andrus' use of password protection, but twice criticizes Dr. Andrus' failure to affirmatively disclaim ownership of, control over, or knowledge regarding the computer. Of course, the computer was located in Ray Andrus' very tiny bedroom, but the majority makes no effort to explain how this does not create an ambiguous situation as to ownership.

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

[10] 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.

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 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.

Notes and Questions

1. *Commentary on Andrus.* Following the *Andrus* decision, the author of these materials offered the following commentary:

> There are two basic ways to search a computer. Digital evidence searches generally occur at both a "logical" or "virtual" level and a "physical" level. The distinction between physical searches and logical searches is fundamental in computer forensics: while a logical search is based on the file systems found on the hard drive as presented by the operating system, a physical search identifies and recovers data across the entire physical drive without regard to the file system.
>
> Most users think of computer searches as occurring at the virtual level, because that's the user experience. But computer forensic software works at the physical level: it treats the hard drive as a physical device that contains millions of zeros and one, not as a virtual "box" of information accessed through an operating system. User profiles and most password protection operate only at a virtual level, so a government forensic analyst operating at a physical level wouldn't even notice the difference unless he was specifically looking for it.
>
> Why does it matter? Well, it matters because the answer to the legal question seems to hinge on whether you apply the Fourth Amendment from a

> virtual perspective or a physical perspective. From a virtual user's perspective, the child pornography was hidden to the father; it was behind a password-protected gate. Under these facts, the father couldn't consent to a search because he would lack common authority over it. From a physical perspective, however, the file was present on the hard drive just like all the other information. Under these facts, the father could consent to the search because he had access rights to the machine generally. The facts hinge on whether you take a physical (external) or virtual (internal) perspective.
>
> The [*Andrus*] Court divided on which perspective to take. The majority (Judge Murphy, joined by the recently-arrived Judge Gorsuch) did not directly address the question of "common authority," relying instead on the "apparent authority" doctrine. Under the apparent authority doctrine, officers can rely on third-party consent if they reasonably conclude that a person has the right to provide consent even if later turns out that he doesn't. This was a sensible move by the majority, because the apparent authority doctrine focuses more on the physical perspective that the officers have rather than a virtual perspective that a user has. Viewed from the physical perspective, the investigators reasonably did not know about the user profile and reasonably believed that the father had rights to consent to that part of the hard drive.
>
> Judge McKay dissented, and instead adopted a virtual perspective. To Judge McKay, the virtual perspective was the only one that mattered: a computer file was a container, and a password-protected computer file was a locked container. Using forensic software to look at a computer from a physical perspective was therefore avoiding the virtual locks. Judge McKay argued that officers should not be allowed to rely on the apparent authority from the physical perspective without first making an inquiry into whether there might be password protection of some kind from a virtual perspective.
>
> I think the majority is probably right, but it's a tremendously interesting case either way. How do you measure the reasonableness of a belief when understandings of what computers are and how they work are so different among typical users and forensic analysts? Should the law follow the understandings of the experts who understand the technology or the general users who don't?

Orin S. Kerr, *Virtual Analogies, Physical Searches, and the Fourth Amendment*, The Volokh Conspiracy, April 26, 2007.

2. *The Order Denying the Petition for Rehearing En Banc.* On August 24, 2007, the Tenth Circuit narrowly denied a petition for rehearing en banc in the *Andrus* case. (Five judges voted for rehearing: McKay, Kelly, Lucero, McConnell, and Holmes.) The two judges in the *Andrus* majority supplemented their opinion with the following additional statement:

> [T]he panel majority notes that its opinion is limited to the narrow question of the apparent authority of a homeowner to consent to a search of a computer on premises in the specific factual setting presented, including the undisputed fact that the owner had access to the computer, paid for internet

access, and had an e-mail address used to register on a website providing access to the files of interest to law enforcement.

Among the questions not presented in this matter, and for which there is no factual development in the record, are the extent of capability and activation of password protection or user profiles on home computers, the capability of EnCase software to detect the presence of password protection or a user profile, or the degree to which law enforcement confronts password protection or user profiles on home computers.

United States v. Andrus, 499 F.3d 1162 (10th Cir. 2007) (denying petition for rehearing en banc).

On pages 423-27 and 438-442, replace Guest v. Leis and United States v. Barr with the following three new cases:

UNITED STATES v. FORRESTER

United States Court of Appeals for the Ninth Circuit, 2007.
495 F.3d 1041.

FISHER, Circuit Judge:

Defendants-appellants Mark Stephen Forrester and Dennis Louis Alba were charged with various offenses relating to the operation of a large Ecstasy-manufacturing laboratory, and were convicted on all counts following a jury trial. They now appeal their convictions and sentences.

Alba challenges the validity of computer surveillance that enabled the government to learn the to/from addresses of his e mail messages, the Internet protocol ("IP") addresses of the websites that he visited and the total volume of information transmitted to or from his account. We conclude that this surveillance was analogous to the use of a pen register that the Supreme Court held in Smith v. Maryland, 442 U.S. 735 (1979), did not constitute a search for Fourth Amendment purposes. Moreover, whether or not the surveillance came within the scope of the then-applicable federal pen register statute, Alba is not entitled to the suppression of the evidence obtained through the surveillance because there is no statutory or other authority for such a remedy.

BACKGROUND

Following a lengthy government investigation, Forrester and Alba were indicted on October 26, 2001, and arraigned shortly thereafter. Forrester was charged with one count of conspiracy to manufacture and distribute 3, 4-methylenedioxymethamphetamine ("Ecstasy") in violation of 21 U.S.C. §§ 841(a)(1), 846. Alba was also charged with that

offense, as well as with engaging in a continuing criminal enterprise in violation of 21 U.S.C. § 848(a), conspiracy to transfer funds outside the United States in promotion of an illegal activity in violation of 18 U.S.C. § 1956(a)(2)(A)(i), (h) and conspiracy to conduct financial transactions involving the proceeds of an illegal activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (h). Both defendants pleaded not guilty to all charges.

During its investigation of Forrester and Alba's Ecstasy-manufacturing operation, the government employed various computer surveillance techniques to monitor Alba's e-mail and Internet activity. The surveillance began in May 2001 after the government applied for and received court permission to install a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet. The mirror port was installed at PacBell's connection facility in San Diego, and enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account. Later, the government obtained a warrant authorizing it to employ imaging and keystroke monitoring techniques, but Alba does not challenge on appeal those techniques' legality or the government's application to use them.

Forrester and Alba were tried by jury. At trial, the government introduced extensive evidence showing that they and their associates built and operated a major Ecstasy laboratory. Witnesses described the lab as "very, very large," and seized documents show that it was intended to produce approximately 440 kilograms of Ecstasy (and $10 million in profit) per month. The government also presented evidence that Alba purchased precursor chemicals for Ecstasy, that Forrester met with a Swedish chemist in Stockholm to learn about manufacturing Ecstasy, that the defendants first tried to construct the lab in two other locations before settling on Escondido, California and that the Escondido lab was located inside an insulated sea/land container and contained an array of devices and chemicals used to make Ecstasy.

The jury convicted Forrester and Alba on all counts. The district court sentenced them each to 360 months in prison and six years of supervised release. Both defendants timely appealed.

. DISCUSSION

[Forrester's appeal is omitted. The following portion of the opinion considers only Alba's Fourth Amendment arguments.]

Alba contends that the government's surveillance of his e-mail and Internet activity violated the Fourth Amendment and fell outside the scope of the then-applicable federal pen register statute.[11] We hold that the surveillance did not constitute a Fourth Amendment search and thus was not unconstitutional. We also hold that whether or not the computer surveillance was covered by the then-applicable pen register statute-an issue that we do not decide-Alba is not entitled to the suppression of any evidence (let alone the reversal of his convictions) as a consequence.

[11] As mentioned earlier, Alba complains only about the initial surveillance through which the government obtained the to/from addresses of his e-mail messages, the IP addresses of the websites that he visited and the total volume of information sent to or from his account. He does not challenge the more intrusive imaging and keystroke monitoring that subsequently took place (though he does argue that the information obtained through those techniques should be suppressed as tainted derivative evidence).

The Supreme Court held in Smith v. Maryland, 442 U.S. 735 (1979), that the use of a pen register (a device that records numbers dialed from a phone line) does not constitute a search for Fourth Amendment purposes. According to the Court, people do not have a subjective expectation of privacy in numbers that they dial because they "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Even if there were such a subjective expectation, it would not be one that society is prepared to recognize as reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Therefore the use of a pen register is not a Fourth Amendment search. Importantly, the Court distinguished pen registers from more intrusive surveillance techniques on the ground that "pen registers do not acquire the contents of communications" but rather obtain only the addressing information associated with phone calls. Id. at 741. See also id. at 743, 99 S.Ct. 2577 ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."); cf. Katz v. United States, 389 U.S. 347 (1967) (legitimate expectation of privacy exists in contents of phone conversation).

Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account.[12] We conclude that these surveillance techniques are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties. Communication by both Internet and telephone requires people to "voluntarily turn[ ] over [information] to third parties." Id. at 744.

Second, e-mail to/from addresses and IP addresses constitute addressing information and reveal no more about the underlying contents of communication than do phone numbers. When the government learns the phone numbers a person has dialed, it may be able to determine the persons or entities to which the numbers correspond, but it does not know what was said in the actual conversations. Similarly, when the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or the particular pages on the websites the person viewed. At best, the government may make educated guesses about

[12] Every computer or server connected to the Internet has a unique IP address. A website typically has only one IP address even though it may contain hundreds or thousands of pages. For example, Google's IP address is 209.85.129.104 and the New York Times' website's IP address is 199.239.137.200. See In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@ xxx. com], 396 F.Supp.2d 45, 48 (D.Mass.2005) (" Pen Register Application ") (citing government application that defined "IP address" as a " 'unique numerical address identifying each computer on the [I]nternet' ").

what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses-but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. The distinction between mere addressing and more content-rich information drawn by the Court in *Smith* and *Katz* is thus preserved, because the computer surveillance techniques at issue here enable only the discovery of addressing information.[13]

The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. See Ex parte Jackson, 96 U.S. 727, 733, (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."). E-mail, like physical mail, has an outside address "visible" to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.

Finally, the pen register in *Smith* was able to disclose not only the phone numbers dialed but also the number of calls made. There is no difference of constitutional magnitude between this aspect of the pen register and the government's monitoring here of the total volume of data transmitted to or from Alba's account. Devices that obtain addressing information also inevitably reveal the amount of information coming and going, and do not thereby breach the line between mere addressing and more content-rich information.

We therefore hold that the computer surveillance techniques that Alba challenges are not Fourth Amendment searches. However, our holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register.

[The Court then considered whether the Pen Register statute was violated, concluding that it was not and that even if it were, there would be no suppression remedy for the violation.] Finally, even if suppression were a valid remedy, any error in not excluding evidence was harmless. The evidence obtained through the computer surveillance was never introduced at trial and was used only as a minor portion of the

---

[13] Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http:// www. nytimes. com, whereas a technique that captures URLs would also divulge the particular articles the person viewed. See Pen Register Application, 396 F.Supp.2d at 49 ("[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. This would reveal content....").

government's application for a court order authorizing imaging and keystroke monitoring. There was more than enough other evidence in that application to generate probable cause even if the to/from addresses of Alba's e-mails, the IP addresses he accessed and the volume of data transmitted to or from his account had been suppressed. The discussion of the computer surveillance spanned only four pages of the 45-page supporting affidavit for the application, and revealed only that Alba had sent e-mails to Forrester and accessed certain chemicals websites. The remainder of the affidavit included extensive -- and more incriminating -- evidence obtained through physical surveillance, conventional pen registers, wiretaps and cooperating witness statements. Much of this other evidence predated the start of the computer surveillance, and there is no indication that evidence obtained through the computer surveillance was used to obtain authorization for any of the other surveillance techniques discussed in the affidavit.

The *Forrester* case addresses non-content information. But what about contents such as e-mails and other remotely stored files? The following decision involves an unusual civil lawsuit brought by a criminal defendant against the United States Government in an effort to block the United States from obtaining e-mail either without first notifying the suspect or by using less process than a warrant. This decision was vacated by the en banc Sixth Circuit on October 9, 2007, and the case presently is still pending before the full Sixth Circuit. Do you think the original panel decision "had it right"?

WARSHAK v. UNITED STATES

United States Court of Appeals for the Sixth Circuit, 2007.
490 F.3d 455, vacated October 9. 2007.

BOYCE F. MARTIN, JR., Circuit Judge.

The government appeals the district court's entry of a preliminary injunction, prohibiting it from seizing "the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order." For the reasons discussed below, we largely affirm the district court's decision, requiring only that the preliminary injunction be slightly modified on remand.

I.

In March 2005, the United States was engaged in a criminal investigation of Plaintiff Steven Warshak and the company he owned, Berkeley Premium Nutraceuticals, Inc. The investigation pertained to allegations of mail and wire fraud, money laundering, and related federal offenses. On May 6, 2005, the government obtained an order from a United States Magistrate Judge in the Southern District of Ohio directing internet service provider ("ISP") NuVox Communications to turn over to government agents information pertaining to Warshak's e-mail account with NuVox. The information to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information pertaining to the customer, including set up, synchronization, etc."; (2) "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak; and (3) "[a]ll Log files and backup tapes." Joint App'x at 49.

The order stated that it was issued under 18 U.S.C. § 2703, part of the Stored Communications Act ("SCA"), and that it was based on "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." The order was issued under seal, and prohibited NuVox from "disclos[ing] the existence of the Application or this Order of the Court, or the existence of this investigation, to the listed customer or to any person unless and until authorized to do so by the Court." The magistrate further ordered that "the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days." On September 12, 2005, the government obtained a nearly identical order pertaining to Yahoo, another ISP, that sought the same types of information from Warshak's Yahoo e-mail account and a Yahoo account identified with another individual named Ron Fricke.

On May 31, 2006, over a year after obtaining the NuVox order, the United States wrote to Warshak to notify him of both orders and their requirements.[14] The magistrate had unsealed both orders the previous day. Based on this disclosure, Warshak filed suit on June 12, 2006, seeking declaratory and injunctive relief, and alleging that the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA. After filing the complaint, Warshak's counsel sought the government's assurance that it would not seek additional orders under section 2703(d) directed at his e-mails, at least for some discrete period of time during the pendency of his civil suit. The government declined to provide any such assurance. In response, Warshak moved for a temporary restraining order and/or a preliminary injunction prohibiting such future searches. The district court held a telephonic hearing on the motions, and eventually granted part of the equitable relief sought by Warshak.

In considering the factors for a preliminary injunction, the district court reasoned that e-mails held by an ISP were roughly analogous to sealed letters, in which the sender

[14] . The government has conceded that it violated the statute by waiting for over a year without providing notice of the e-mail seizures to Warshak or seeking extensions of the delayed notification period, and it appears to have violated the magistrate's decision for the same reason.

maintains an expectation of privacy. This privacy interest requires that law enforcement officials obtain a warrant, based on a showing of probable cause, as a prerequisite to a search of the e-mails. Because it viewed Warshak's constitutional claim as meritorious, the district court deemed it unnecessary to examine his likelihood of success on the SCA claim. It also found that Warshak would suffer irreparable harm based on any additional constitutional violations, that such harm was imminent in light of the government's past violations and its refusal to agree not to conduct similar seizures in the future, that Warshak lacked an adequate remedy at law to protect his Fourth Amendment rights, and that the public interest in preventing constitutional violations weighed in favor of the injunction. The district court also made clear that further factual development would be necessary for a final disposition, and that the injunction was tailored to protect Warshak from constitutional violations in the interim.

The district court rejected the full scope of Warshak's request to enjoin the government from seizing any of his e-mails in the future. It stated that it was not "presently prepared to hold that 18 U.S.C. § 2703(d) facially violates the Fourth Amendment by simple virtue of the fact that it authorizes the seizure of personal e-mails from commercial ISPs without a warrant and on less than a showing of probable cause." D. Ct. Op. at 16-17. The statute's authorization of this procedure based only on the government's ex parte representations struck the district court as more problematic, however, and it held that the "combination of a standard of proof less than probable cause and potentially broad ex parte authorization cannot stand." Id. at 17. As a result, it deemed the constitutional flaws of the statute "facial in nature," and agreed to preliminarily enjoin additional seizures of e-mails from an ISP account of any resident of the Southern District of Ohio without notice to the account holder and an opportunity for a hearing.

The gist of this remedy appears to be that when a hearing is required and the e-mail account holder is given an opportunity in court to resist the disclosure of information, any resulting order is more like a subpoena than a search warrant. Therefore the standard necessary to obtain an order under the SCA-that the government introduce "specific and articulable facts showing that there are reasonable grounds to believe that the contents" of the e-mail to be seized "are relevant and material to an ongoing criminal investigation"-is permissible as the functional equivalent of a subpoena given the subject's ability to contest the order in court. Because this standard is lower than the probable cause standard necessary to obtain a search warrant, it is sufficient to justify a warrantless search only in instances where notice is provided to the account holder.

The government appeals from the district court's ruling.

II.

The SCA, passed by Congress in 1986, is codified at 18 U.S.C. §§ 2701 to 2712, and contains a number of provisions pertaining to the accessibility of "stored wire and electronic communications and transactional records." Portions of the SCA that are not directly at stake here prohibit unauthorized access of electronic communications (§ 2701) and prohibit a service provider from divulging the contents of electronic communications that it is storing for a customer with certain exceptions pertaining to law enforcement needs (§ 2702). At issue in this case is § 2703, which provides procedures through which

a governmental entity can access both user records and other subscriber information, and the content of electronic messages.

Subsection (a) requires the use of a warrant to access messages that have been in storage for 180 days or less. Subsection (b) provides that to obtain messages that have been stored for over 180 days, the government generally must either (1) obtain a search warrant, (2) use an administrative subpoena, or (3) obtain a court order. The latter two require prior notice to the subscriber, allowing the subscriber an opportunity for judicial review before the disclosure. 18 U.S.C. § 2703(b). The final subsection cited here contains the exception to the requirement that the government must either provide notice to the subscriber if seeking either an SCA order or an administrative subpoena, or must, in the absence of notice, obtain a search warrant. This exception, which allows for delayed notice under section 2705, is the root of the present controversy.

Subsection (d), which is referenced in subsection (b), sets forth the procedure and requirements for obtaining a court order (as opposed to a warrant). 18 U.S.C. § 2703(d). The parties agree that the standard of proof for a court order-"specific and articulable facts showing that there are reasonable grounds to believe that the contents ... or records ... are relevant and material to an ongoing criminal investigation"-falls short of probable cause.

Section 2705 . . . provides for delayed notice of a 2703(d) court order. . . . . Subsection (b) of section 2705 similarly allows the government to obtain a court order prohibiting the ISP from notifying the account holder "of the existence of the warrant, subpoena, or court order," when the government is not required to provide him notice. These provisions of sections 2703 and 2705 largely govern the seizures of Warshak's e-mails.

The injunctive relief imposed by the district court has a specific narrow application to portions of the SCA. It would still allow seizures of e-mails pursuant to a warrant or with prior notice to a subscriber. The portions that it enjoins are the exception provided in section 2703(b)(1)(B)(ii), which allows for a court order with delayed notice to the account holder, and the procedures provided in section 2705, which are incorporated by reference into section 2703(b)(1)(B)(ii).

III.

The government focuses on four issues in challenging the preliminary injunction. First, it argues that Warshak's claims are not justiciable in the first instance, based on the doctrines of standing and ripeness. Second, it contends that the Fourth Amendment's probable cause standard is inapplicable in the context of SCA seizures, which it likens to compelled disclosures. This issue primarily covers Warshak's likelihood of success on the merits, the first factor in the preliminary injunction analysis. Next, it argues that Warshak's claims are not the proper subject of a facial challenge to the provisions of the SCA in question. Finally, it challenges the district court's balancing of the remaining preliminary injunction factors.

[Discussions of standing and ripeness are omitted.]

1. Probable Cause versus Reasonableness

With respect to the merits of the preliminary injunction, the government argues that court orders issued under section 2703 are not searches but rather compelled disclosures, akin to subpoenas. As a result, according to the government, the more stringent showing of probable cause, a prerequisite to the issuance of a warrant under the Fourth Amendment, is inapplicable, and an order under section 2703 need only be supported by a showing of "reasonable relevance."

The government is correct that "whereas the Fourth Amendment mandates a showing of probable cause for the issuance of search warrants, subpoenas are analyzed only under the Fourth Amendment's general reasonableness standard." Doe v. United States, 253 F.3d 256, 263-64 (6th Cir.2001). As this Court has explained, "[o]ne primary reason for this distinction is that, unlike 'the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant[,]' the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced." Id. at 264 (quoting In Re Subpoena Duces Tecum, 228 F.3d 341, 347-49 (4th Cir.2000). The government is also correct that this principle extends to subpoenas to third-parties-that is, entities other than the subject of the investigation, like NuVox and Yahoo in this case. See United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir.1993).

Phibbs makes explicit, however, a necessary Fourth Amendment caveat to the rule regarding third-party subpoenas: the party challenging the subpoena has "standing to dispute [its] issuance on Fourth Amendment grounds" if he can "demonstrate that he had a legitimate expectation of privacy attaching to the records obtained." Id. This language reflects the rule that where the party challenging the disclosure has voluntarily disclosed his records to a third party, he maintains no expectation of privacy in the disclosure vis-a-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities.

Combining this disclosure to a third party with the government's ability to subpoena the third party alleviates any need for the third-party subpoena to meet the probable cause requirement, if the challenger has not maintained an expectation of privacy with respect to the individual being compelled to make the disclosure. For example, in *Phibbs*, the documents in question were credit card and phone records that were "readily accessible to employees during the normal course of business." 999 F.2d at 1078. A similar rationale was employed by the Supreme Court in Miller. 425 U.S. at 442. The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure-in this instance, the ISPs. If he does not, as in *Phibbs* or *Miller*, then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure.

2. Reasonable expectation of privacy in e-mail content

Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, recognized by the Supreme Court in its line of cases involving government eavesdropping on telephone conversations. See Smith v. Maryland, 442 U.S. 735 (1979);

Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967). In *Berger* and *Katz*, telephone surveillance that intercepted the content of a conversation was held to constitute a search, because the caller "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and therefore cannot be said to have forfeited his privacy right in the conversation. *Katz*, 389 U.S. at 352, 88 S.Ct. 507. This is so even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment." *Smith*, 442 U.S. at 746, 99 S.Ct. 2577 (Stewart, J., dissenting). On the other hand, in *Smith*, the Court ruled that the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications." 442 U.S. at 741, 99 S.Ct. 2577 (emphasis in original).

The distinction between *Katz* and *Miller* makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another. First, we must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded. Clearly, under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search. It is true, however, that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. See *Miller*, 425 U.S. at 443, 96 S.Ct. 1619 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.

The second necessary inquiry pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained. This distinction provides the obvious crux for the different results in *Katz* and *Smith*, because although the conduct of the telephone user in *Smith* "may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." 442 U.S. at 743, 99 S.Ct. 2577. Like the depositor in *Miller*, the caller in *Smith* "assumed the risk" of the phone company disclosing the records that he conveyed to it. Yet this assumption of the risk is limited to the specific information conveyed to the service provider, which in the telephone context excludes the content of the conversation. It is apparent, therefore, that although the government can compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other

hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).

This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber's Fourth Amendment interest under *Smith*, because like the information obtained through the pen register in *Smith* and like the bank records in *Miller*, subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-a-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems. The combined precedents of *Katz* and *Smith*, however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

Similarly, under both *Miller* and Katz, if the government in this case had received the content of Warshak's e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-a-vis his e-mailing partners. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz*. Thus, as Warshak argues, the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs*, postal workers would not be expected to read the letter in the normal course of business. Similarly, a bank customer maintains an expectation of privacy in a safe deposit box to which the bank lacks access[15](as opposed to bank records, like checks or account statements) and the government could not compel disclosure of the contents of the safe deposit box only by subpoenaing the bank.

This analysis is consistent with other decisions that have addressed an individual's expectation of privacy in particular electronic communications. In Guest v. Leis, 255 F.3d 325, 333 (6th Cir.2001), we concluded that users of electronic bulletin boards lacked an expectation of privacy in material posted on the bulletin board, as such materials were "intended for publication or public posting." Of course the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients. Although we stated that an e-mail sender would "lose a legitimate expectation of privacy in an e-mail that had already reached its recipient," analogizing such an e-mailer to "a letter-writer," this diminished privacy is only relevant with respect to the recipient, as the sender has assumed the risk of disclosure by or through the recipient. Guest did not hold that the mere use of an intermediary such as an ISP to send and receive e-mails amounted to a waiver of a legitimate expectation of privacy.

[15] See United States v. Thomas, No. 88-6341, 1989 WL 72926, at *2, 1989 U.S.App. LEXIS 9628, at *6 (6th Cir. July 5, 1989) ("Citizens have legitimate expectations of privacy in the contents of their safe deposit boxes.").

Other courts have addressed analogous situations where electronic communications were obtained based on the sender's use of a computer network. In *United States v. Simons,* 206 F.3d 392, 398 (4th Cir. 2000), the Fourth Circuit held that a government employee lacked a reasonable expectation of privacy in electronic files on his office computer, in light of the employer's policy that explicitly notified the employee of its intention to "audit, inspect, and monitor," his computer files. In light of this explicit policy, the employee's belief that his files were private was not objectively reasonable. On the other hand, in United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir.2007), the Ninth Circuit held that a university student did have a reasonable expectation of privacy in his computer files even though he "attached [his computer] to the university network," because the "university policies do not eliminate Heckenkamp's expectation of privacy in his computer." Although the university did "establish limited instances in which university administrators may access his computer in order to protect the university's systems," this exception fell far short of a blanket monitoring or auditing policy, and the Ninth Circuit deemed it insufficient to waive the user's expectation of privacy.

Heckenkamp and *Simons* provide useful bookends for the question before us, regarding when the use of some intermediary provider of computer and e-mail services-be it a commercial ISP, a university, an employer, or another type of entity-amounts to a waiver of the user's reasonable expectation of privacy in the content of the e-mails with respect to that intermediary. In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited as in *Simons,* the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy, as in *Heckenkamp*.

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user "seeks to preserve as private," and therefore "may be constitutionally protected." *Katz,* 389 U.S. at 351, 88 S.Ct. 507. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past. See *Katz,* 389 U.S. at 352, 88 S.Ct. 507 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.")

The government asserts that ISPs have the contractual right to access users' e-mails. The district court's ruling was based on its willingness to credit Warshak's contrary factual argument that "employees of commercial ISPs [do not] open and read-[nor do] their subscribers reasonably expect them to open and read-individual subscriber e-mails as a matter of course." D. Ct. Op. at 10-11. This factual determination tracks the language from *Miller* and *Phibbs* that suggests a privacy interest in records held by a third party is only undermined where the documents are accessed by the third party or its employees "in the ordinary course of business." *Miller,* 425 U.S. at 442, 96 S.Ct. 1619. Moreover, as explained in the Ninth Circuit's decision in *Heckenkamp,* mere accessibility

is not enough to waive an expectation of privacy. See *Heckenkamp*, 482 F.3d at 1147 (holding that university policies establishing "limited instances in which university administrators may access [the user's] computer in order to protect the university's systems" was insufficient to eliminate an expectation of privacy).

Where a user agreement calls for regular auditing, inspection, or monitoring of e-mails, the expectation may well be different, as the potential for an administrator to read the content of e-mails in the account should be apparent to the user. Where there is such an arrangement, compelled disclosure by means of an SCA order directed at the ISP would be akin to the third party subpoena directed at a bank. . . . In contrast, the terms of service in question here, which the government has cited to in both the district court and this Court, clearly provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails. Because the ISPs right to access e-mails under these user agreements is reserved for extraordinary circumstances, much like the university policy in *Heckenkamp*, it is similarly insufficient to undermine a user's expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by ISPs, or that users are aware of such access of content.

The government also insists that ISPs regularly screen users' e-mails for viruses, spam, and child pornography. Even assuming that this is true, however, such a process does not waive an expectation of privacy in the content of e-mails sent through the ISP, for the same reasons that the terms of service are insufficient to waive privacy expectations. The government states that ISPs "are developing technology that will enable them to scan user images" for child pornography and viruses. The government's statement that this process involves "technology," rather than manual, human review, suggests that it involves a computer searching for particular terms, types of images, or similar indicia of wrongdoing that would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient. But the reasonable expectation of privacy of an e-mail user goes to the content of the e-mail message. The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages. The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send.

The government's compelled disclosure argument is initially on point, but fails to address adequately the caveat relating to a party's maintenance of a reasonable expectation of privacy in documents in the custody of a third party. A warrant based on probable cause would not have been necessary had the government subpoenaed Warshak or given him prior notice of its intent to seek an SCA order, because the need for this higher showing would be offset by his ability to obtain judicial review before producing any e-mails. The same rationale would apply if the government subpoenaed a third party that had access to the content of the e-mails, and against whom Warshak had no claim of privacy, such as the recipient of one of his e-mails. By the same token, an SCA order that provided notice to the ISP alone, and not to the user, would be appropriate in the limited instances where the user had waived his expectation of privacy with respect to the ISP, such as where the government can show that auditing, monitoring, or inspection are

expressly provided for in the terms of service, or where the user has e-mailed content directly to the ISP. Where the third party is not expected to access the e-mails in the normal course of business, however, the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement.

The district court enjoined the United States "from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard...." D. Ct. Op. at 19. Our discussion above necessitates one modification to this injunction, which counsel for Warshak agreed at oral argument would be appropriate. If the government can show, based on specific facts, that an e-mail account holder has waived his expectation of privacy vis-a-vis the ISP, compelled disclosure of e-mails through notice to the ISP alone would be appropriate. This is a narrow modification, however, as a right to access e-mails in an account only in certain limited circumstances would not be sufficient. Rather, the government must show that the ISP or other intermediary clearly established and utilized the right to inspect, monitor, or audit the content of e-mails, or otherwise had content revealed to it. In such cases the SCA order will operate as the functional equivalent of a third party subpoena, allowing disclosure through a party that has total access to the documents in question.

On remand, therefore, the preliminary injunction shall allow seizures of e-mail in three situations: (1) if the government obtains a search warrant under the Fourth Amendment, based on probable cause and in compliance with the particularity requirement; (2) if the government provides notice to the account holder in seeking an SCA order, according him the same judicial review he would be allowed were he to be subpoenaed; or (3) if the government can show specific, articulable facts, demonstrating that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity, in which case compelled disclosure may occur if that entity is afforded notice and an opportunity to be heard.

. . . .

The government also argues that by reserving the right to screen e-mails, the ISPs diminish any expectation of privacy their subscribers might have. Again, it is entirely possible, if not likely, that this process occurs without ever having a human being read the content of subscribers' e-mails. Where total access is the norm, we hold that the government may show as much and then may compel disclosure through the ISP. Less in-depth screening, however, is insufficient to diminish the privacy interest in an e-mail account.

As another example, the government contends that when an e-mail account is abandoned, as could occur with ISPs that require payment which the user fails to remit, the account holder maintains no reasonable expectation of privacy. The government analogizes this situation to a hotel room, in which the guest has an expectation of privacy, but abandons it when he leaves the room or is evicted by management. See, e.g., United States v. Allen, 106 F.3d 695, 699 (6th Cir.1997). This analogy lacks any connection to the actual practices of commercial ISPs. When a hotel guest checks out of his room,

another person will occupy it, access every part of it in which he might have maintained any privacy interest, put his underwear in the same drawer, and otherwise extinguish any privacy interest to the fullest extent. Dominion and control over the hotel room is entirely surrendered to the hotel management, which in turn passes it on to the next guest who occupies the room. On the other hand, when an e-mail user stops using an e-mail address that is tied to his personal identity, he would certainly not expect that somebody else could come along, sign up for the same account, and not only send e-mails in his name, but read every past e-mail that he had failed to delete from the account or sent to someone else. There is no reason to believe that dominion or control over the contents of the account is yielded to the ISP or another user. This analogy is entirely inapposite.

Finally, the government points to "e-mail accounts that are procured through fraudulent means" as situations where an account holder has no reasonable expectation of privacy. This argument is another red herring, primarily because it cannot account for the majority of commercial e-mail services that offer their services for free. This obviously begs the question of why someone would have to commit fraud to get an account. Yet even if a hypothetical user wanted to conceal his identity or address from the ISP, the provision of misinformation would not bear in any way upon the privacy of the content of the user's e-mails. Further, the government suggests that a "hacker" who obtains "Internet services and e-mail accounts using stolen credit cards" would lack an expectation of privacy in the account he purchases, citing to a case where the thief of a stolen laptop did not have an expectation of privacy in material on the computer's hard drive. See United States v. Caymen, 404 F.3d 1196, 1201 (9th Cir.2005).

Where a thief steals someone else's property, it is true that he lacks an expectation of privacy in that property, such as the laptop computer at issue in Caymen. The government's hypothetical thief in this case would clearly not have an expectation of privacy in the victim's credit card account, which he illegally accessed. Why this person would lack a reasonable expectation of privacy in the contents of an e-mail account, however, is far from clear. Because the government's hypothetical "hackers" cannot be said to "steal" the contents of the e-mails in the account, or an entire ISP server for that matter, this example is also unhelpful.

The district court correctly determined that e-mail users maintain a reasonable expectation of privacy in the content of their e-mails, and we agree that the injunctive relief it crafted was largely appropriate, although we find necessary one modification. On remand, the preliminary injunction should be modified to prohibit the United States from seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 18 U.S.C. § 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard.

Notes and Questions

1. What is the holding of Warshak? The *Warshak* opinion is quite complicated because the Court attempted to identify all of the Fourth Amendment rules that would govern every access to e-mail. What are those rules? Here is one attempt at a summary:

(a) When the government seeks to compel the contents of personal e-mails from an Internet service provider, it may obtain the e-mail from the Internet service provider only in the following circumstances:

(1) Pursuant to a subpoena, if the government can establish, "based on specific facts," "that the ISP or other intermediary clearly established and utilized the right to inspect, monitor, or audit the contents, or otherwise had content revealed to it," or:

(2) Pursuant to a subpoena, if the government provides prior notice to the e-mail subscriber and permits the subscriber an opportunity to challenge the constitutional reasonableness of the subpoena before the e-mails are disclosed, or:

(3) Pursuant to a search warrant based on probable cause that "target[s] e-mails that could reasonably be believed to have some connection to its specific investigation," if neither the circumstances in subsections (1) or (2) are satisfied.

(b) Subsection (a) shall not apply to computer scanning of e-mail for key words, types of images or "similar indicia of wrongdoing" in a way that does not disclose contents to an actual person

Is this an accurate summary of the *Warshak* opinion? If so, is it sensible as a matter of policy? Is it plausible as a matter of Fourth Amendment law?

2. Although the *Warshak* opinion was later vacated en banc, its core holding of Fourth Amendment protection in remotely stored contents is reflected in the following case.

UNITED STATES v. D'ANDREA

United States District Court for the District of Massachusetts, 2007.
497 F.Supp.2d 117.

STEARNS, District Judge.

The underlying facts are sordid and need not be elaborated beyond their essentials. The case began with an anonymous call on December 2, 2004, to a Department of Social Services (DSS) child abuse hotline.[16] The caller reported that Jane Doe, the eight-year old daughter of defendant Kendra D'Andrea, was being sexually abused by her mother and the mother's live-in boyfriend, defendant Willie Jordan. The caller also stated that pictures of Jordan performing oral sex on the girl had been posted on a Sprint PCS website. The caller provided the address of D'Andrea's apartment, the log-in name and password for the website, and the number of a cellular telephone used by defendants.

[16] The identity of the caller is known to the parties. While she did not give her name, she identified herself to the hotline operator as a former girlfriend and the mother of one of defendant Willie Jordan's children. She is identified by name in defendants' pleadings.

Jerome Curley, a senior administrator at DSS, who was notified of the call, was able to access the website. After confirming the caller's description of the posted images, he downloaded and printed them. DSS then notified the Gloucester police. Joseph Fitzgerald, a Gloucester police detective, used the images to obtain a warrant for the search of D'Andrea's apartment from a local clerk-magistrate. The warrant was executed shortly after midnight. The searching officers found D'Andrea, two young children (including Jane Doe), and a mobile camera telephone. D'Andrea was then taken into custody. After being advised of her *Miranda* rights, she confessed. She admitted to the sexual abuse of Jane Doe and to the posting of the images on the website. She also stated that when Jordan was away on business, she would blindfold the child, pose her in a provocative manner, and transmit the sexually-charged images to Jordan via the mobile camera telephone.

D'Andrea and Jordan now move to suppress the downloaded images,[17] the evidence seized from [the apartment], and any incriminating statements made by D'Andrea and Jordan. Defendants allege that Curley (the DSS supervisor) violated their Fourth Amendment rights by accessing the Sprint PCS website and downloading the images. As the images were critical to the clerk-magistrate's finding of probable cause, defendants argue that the fruits of the search of D'Andrea's apartment as well as her subsequent confession should be suppressed as the harvest of a poisonous tree.

DISCUSSION

Privacy analysis consists of a two-part inquiry. First, did a defendant manifest a subjective expectation of privacy in the searched premises or property? Second, is that expectation one that society is prepared to recognize as objectively reasonable? The reasonableness of an asserted interest in privacy is determined by the totality of the circumstances.

Both D'Andrea and Jordan state that because the Sprint PCS website was password-protected, they believed that what was posted on the site was a private matter that was exclusively theirs to share, and that they therefore had a subjective expectation of privacy in the website's contents. Assuming that this is true -- it would be somewhat astonishing if it were not -- the question still remains whether this expectation is one that society would recognize as reasonable.

Professor Warren LaFave, a preeminent authority on the Fourth Amendment, argues that a person who avails herself of a website's password protection should be able to claim a reasonable expectation of privacy in the site's contents. Professor LaFave makes the point that while a service provider has a need to access information regarding the identity of a site holder and the volume and extent of her usage, it has no legitimate reason to inspect the actual contents of the site, anymore than the postal service has a legitimate interest in reading the contents of first class mail, or a telephone company has a legitimate interest in listening to a customer's conversations. "Reliance on protections such [as] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms,

[17] At Jordan's request, Sprint removed the images from the website before a preservation letter could be served by police. Consequently, the DSS copies of the images are all that remain.

even though each form of protection is penetrable."[18] LaFave, 1 Search and Seizure § 2.6 at 721 (4th ed.2006). Professor LaFave's argument is persuasively echoed in Warshak v. United States, 490 F.3d 455 (6th Cir.2007). [Extensive quotations from *Warshak* deleted.]

The protections of the Fourth Amendment, it must be emphasized, apply only to the actions of the State and its agents. Where the State is simply the passive recipient of evidence gathered by a private party acting without the State's instigation or direction, a defendant incriminated by that evidence has no recourse to the Fourth Amendment. . . . . Defendants make no argument -- nor could one credibly be made -- that the anonymous caller was acting as an agent of the State in reporting the abuse of Jane Doe to DSS. The argument rather is that the DSS administrator (Curley) who accessed the website and downloaded the images of the abuse violated defendants' Fourth Amendment rights.

This argument fails for the simple reason that Curley intruded no further into defendants' zone of privacy than did the anonymous caller. Where a private party, acting on his or her own, searches a closed container, a subsequent warrantless search of the same container by government officials does not further burden the owner's already frustrated expectation of privacy. United States v. Jacobsen, 466 U.S. 109, 117 (1984). "The additional invasions of [a defendant's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." Id. at 115. Moreover, where an expectation of privacy in an item has been effectively destroyed by a private search, police do not violate the Fourth Amendment by examining the same item more thoroughly or with greater intensity so long as they do not "significantly expand" upon or "change the nature" of the underlying private search. United States v. Runyan, 275 F.3d 449, 464-465 (5th Cir. 2001).

At day's end, this case falls clearly into the "assumption of the risk" exception identified in *Warshak* and Supreme Court precedent.[19] "It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." *Jacobsen*, 466 U.S. at 117. Thus, even granting defendants a reasonable expectation of privacy in the graphic website images of Jane Doe, by sharing the website access information with the anonymous caller, defendants took the risk that their right to privacy in the website's contents could be compromised.

For the foregoing reasons, the motion to suppress physical evidence is denied.

---

[18] Professor LaFave acknowledges that when telephone access to a website is possible, more difficult issues are raised. LaFave, 1 Search and Seizure § 2.6 at 716 (4th ed.2006). The premise of Professor LaFave's argument -- that a service provider has no legitimate reason to monitor the contents of an internet site -- may not be as rock solid as it appears. See Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir.2003) (acknowledging the possibility that the "Good Samaritan" provision of the Communication Decency Act of 1996, 47 U.S.C. § 230(c), might not have preemptive effect on a state law imposing a duty on ISP providers to filter offensive content on hosted websites).

[19] D'Andrea states in her affidavit that she never gave the password to anyone and that she "thought" the same was true of Jordan. Jordan states in his affidavit that he never "voluntarily" gave the website information to anyone else. As the government persuasively argues, the "anonymous" caller could have learned the information from no one other than one (or both) of the defendants.

Notes and Questions

1. Should a person always have a reasonable expectation of privacy in password protected files? Or should that expectation of privacy depend on circumstances such as terms of service, compliance with contractual terms, the location of the server, or other details about the case?

2. Was the *D'Andrea* court correct that the access to the protected files fell within an exception to the warrant requirement? The private search doctrine lets the police reconstruct the search undertaken by a private actor; the private actor can in effect show the police what she saw without invading a Fourth Amendment right. But how much evidence was there that the police merely reconstructed the private person's search? Do we know what the private person saw or in what circumstances? Do we even know if she searched the computer at all? Judge Stearns relies on the *Runyan* case from the Fifth Circuit, discussed in the main casebook at p. 307, which held that a private party viewing one file on a computer eliminated a reasonable expectation of privacy with respect to *all* the files. But is that persuasive? And do we even know that the private person saw one file in the account?

Finally, consider Judge Stearns' discussion of the "assumption of the risk" doctrine. The caller, who turned out to be the man's ex-girlfriend, knew the username and password. But we don't know how she knew it. Assuming she was given rights to access the account, we don't know if there were some kind of conditions placed on her access. Judge Stearns appears to assume that the defendants must have given her the account and password and given her full access rights. But there are other possibilities: there are ways of finding out someone's username and password without them giving it to you and giving you full access rights to an account. Why do you think Judge Stearns made the assumptions that he made? Are his assumptions persuasive?

CHAPTER 6:
STATUTORY PROTECTIONS

On page 509, after Note 3, add the following new Note:

3.1. In *United States v. Standefer*, 2007 WL 2301760 (S.D. Cal. 2007), a district court considered whether the government had violated Section 2703 by obtaining account records from e-gold, an online payment system that is similar to PayPal, using an administrative subpoena. The Court held that e-gold was not a provider of ECS nor RCS and therefore that Section 2703 was not implicated:

> e-gold is not a provider of electronic communication services. . . . The Court concludes that e-gold is not a service which provides users the ability to send or receive electronic communications, rather e-gold is a service which utilizes the ability to send or receive electronic communications to permit the instant transfer of gold ownership between its users. Therefore, the Government was not required by § 2703(a) to utilize a warrant to obtain the requested information from e-gold.
>
> Similarly, . . . e-gold is [not] a provider of . . . a remote computing service. . . . The term "remote computing service" is defined by 18 U.S.C. § 2711(2) as the "provision to the public of computer storage or processing services by means of an electronic communications system." The Senate explained the term "remote computing service," as used in the Stored Communications Act:
>
> > In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes -- hospitals, banks and many others -- use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.
>
> S.Rep. No. 99-541, at 10-11 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3564-64.
>
> The Court concludes that e-gold provides neither computer storage nor processing services, as those terms are used in § 2711(2), to the public.

> Cf. Quon v. Arch Wireless Operating Co., Inc., 445 F.Supp.2d 1116, 1130-37 (C.D.Cal.2006) (concluding that wireless communications provider that stored and retrieved text messages for its subscribers was a remote computing service); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 Geo. Wash. L. Rev. 1208, 1229-30 (2004) (concluding that eBay is not a remote computing service because "[t]he legislative history indicates that 'processing services' refer to outsourcing functions.... This seems quite different from eBay: a user does not outsource tasks to eBay but rather uses eBay as a destination for the user's requests concerning buying and selling items."). A client of e-gold does not outsource tasks, but rather uses e-gold to transfer gold ownership to other users. Neither does an e-gold customer use e-gold to simply store electronic data.

Id. at *4-*5.

CHAPTER 7:
JURISDICTION

On the middle of page 604, add the following case:

How does the Fourth Amendment apply to searches occurring abroad pursuant to Mutual Legal Assistance Treaties or Letters Rogatory? That issue recently arose in a white collar crime case involving an alleged fraud scheme run by two bankers who were U.S. citizens but had offices in London. The United States government issued a request pursuant to the U.S./U.K. Mutual Legal Assistance Treaty for the U.K. authorities to execute a search of the offices in the U.K. The defendants then brought a Fourth Amendment challenge to the resulting search.

UNITED STATES v. VILAR

United States District Court for the Southern District of New York, 2007.
2007 WL 1075041.

KARAS, J.

Defendants Alberto William Vilar and Gary Alan Tanaka are charged with an alleged fraud scheme involving investors' funds. The Superseding Indictment, filed on August 15, 2006, charges Defendants with conspiracy to commit securities, mail, wire, and investment advisor fraud and money laundering. They are also charged in separate substantive counts with securities fraud, investment advisor fraud, mail fraud, two counts of wire fraud, and four counts of money laundering.

Each Defendant has filed a Motion to Suppress the fruits of . . [a search of the offices of a business "Amerindo U.K."] conducted at the Government's request, pursuant to a Mutual Legal Assistance Treaty and two U.K. search warrants, in the United Kingdom on October 13 and 14, 2005. The motions to suppress the U.K. search are denied.

I.

Detective Sergeant Shaw is a 23-year veteran of the Metropolitan Police in London, England, who has spent much of his law enforcement career investigating white collar crime. At the time of the contested search, Detective Sergeant Shaw was assigned to the International Assistance Unit. Among other things, this Unit processes foreign evidence requests made of the United Kingdom through a Mutual Legal Assistance Treaty ("MLAT"). It is pursuant to such a treaty, for example, that a foreign government agency can request that United Kingdom law enforcement officials conduct a search of a business premises. According to Detective Sergeant Shaw, any such request must come from the proper authority and otherwise comport with the terms of the particular MLAT. Among other such terms, the U.K.'s MLATs require that the requested search be part of an investigation of conduct that is a crime under British law. A MLAT request to search a premises is first reviewed by the United Kingdom Central Authority ("UKCA"), which

vets the request to determine if it comports with the MLAT and British law. If the request is satisfactory, it then is assigned to the appropriate U.K. law enforcement agency.

Detective Sergeant Shaw testified that when he receives a MLAT request to conduct a search from the UKCA, he first reviews the request to determine if the request, in his view, is based on sufficient information to justify a warrant. In his experience, he has rejected many requests for a search at this stage of the process. If, however, the request appears to be substantiated, Detective Sergeant Shaw then conducts a background inquiry by, for example, investigating the target premises. Once Detective Sergeant Shaw determines that the request is in order and completes his own inquiry, Detective Sergeant Shaw then awaits a "direction" from the Home Office specifically authorizing him to conduct the search. From there, U.K. law requires Detective Sergeant Shaw to submit his search warrant request to a senior police officer unconnected to the investigation. This is yet another stage where the request can be rejected. If, however, the senior officer approves the search request, then Detective Sergeant Shaw formally applies for the search warrant through the "clerk of the Court," a court staff person who advises his view of the validity of the warrant. According to Detective Sergeant Shaw, it is not uncommon for the court clerk to recommend rejecting a search warrant request. If, however, the clerk recommends approval of the warrant, the clerk will initial the request and make arrangements for the Detective Sergeant to formally apply for the warrant before the duty judge.

Detective Sergeant Shaw testified that he was the Metropolitan Police official who was assigned the American government's request to conduct a search of Amerindo U.K.'s premises. According to Detective Sergeant Shaw, he received a telephone call from the UKCA in July 2005 regarding an urgent request from American law enforcement officials to search the business premises of Amerindo, U .K. Following the procedure he had described, Detective Sergeant Shaw reviewed the MLAT request to determine if there was a valid basis to apply for a search warrant of Amerindo's business premises. In his words, he believed the request to be "comprehensive and sound." (Tr. 228, May 31, 2006.)

The search warrant application consisted of a template application that Detective Sergeant Shaw filled in, a typed rider that came directly from the MLAT request, and the information in support of the warrant application which Shaw typed himself. . . .

Upon arriving at Bow Street Magistrate's Court, Detective Sergeant Shaw handed the application to Mrs. Elizabeth Franey, a senior legal adviser at the court with approximately twenty years of experience. . . . . Approximately five hours later, Detective Sergeant Shaw returned to the Bow Street Magistrate's Court hoping to be able to make his application to a judge. Mrs. Franey informed him that she had reviewed the application and passed it to a judge, thereby indicating her approval of the application. Then Detective Sergeant Shaw made his application to the senior district judge at the court, Timothy Workman, who was the "duty judge" that day. Judge Workman is the most senior district judge in England and Whales, with the power to issue Schedule I orders and warrants.

Judge Workman asked Detective Sergeant Shaw a series of questions including questions about the nature of the premises, whether the search would extend beyond Amerindo U.K.'s eight crates, the anticipated length of the search, the nature of the property where the materials had previously been located, and whether that property had

been shared. . . . Judge Workman then stated that he was satisfied with the application, which was kept at the court, and signed the warrant. Detective Sergeant Shaw believed he was then in possession of a lawfully-obtained, lawfully-issued warrant.

After obtaining the warrant, Detective Sergeant Shaw met with the American authorities, including Inspector Fraterrigo. At that meeting, Detective Sergeant Shaw explained that the warrant had been granted, and consequently that the Americans had not wasted their trip over. They then discussed their respective roles during the execution of the search. Detective Sergeant Shaw explained that the Americans were entitled to assist in the search, but that they remained under British supervision and that the ultimate decision regarding whether to seize particular items would rest with the British authorities.

The warrant signed by Judge Workman was executed on Thursday, October 13, 2005.

II.

Defendants claim that the U.K. search was invalid because it was not executed pursuant to a valid warrant issued by a United States judicial officer, and was otherwise unreasonable. Defendants' train of logic is as follows: (1) American officials are required to comport their investigative activities with the Bill of Rights; (2) the Bill of Rights governs the conduct of American officials even when they operate abroad; (3) there is caselaw applying the Bill of Rights and the Fourth Amendment to extraterritorial conduct by or on behalf of American officials; and (4) because there was no warrant signed by an American judicial officer based on an individualized showing of probable cause that Defendants violated American laws, the U.K. search executed by Metropolitan Police officers at the American Government's request was "warrantless," even though it was conducted pursuant to two warrants signed by U.K. judicial officials.

The missing link in Defendants' chain is any authority holding that the Warrant Clause of the Fourth Amendment applies to extraterritorial searches conducted by, or at the request of, American Government officials. While neither the Supreme Court nor the Second Circuit has squarely addressed the issue, the Supreme Court has strongly hinted that it takes a dim view of the suggestion that the Warrant Clause applies to extraterritorial searches. In fact, the Supreme Court discussed the reach of the Fourth Amendment to extraterritorial searches while reversing the very case cited by Defendants in support of their claim. The Defendants cite to the Ninth Circuit's opinion in United States v. Verdugo-Urquidez, 856 F.2d 1214, 1230 (9th Cir. 1988), which stated that "we cannot relieve the government from its obligation to obtain a search warrant simply because the place to be searched by the government is outside this country. To do so would be to treat foreign searches differently from domestic searches just because they are foreign." While Defendants acknowledge that the Supreme Court reversed the Ninth Circuit in *Verdugo-Urquidez*, they claim that the Supreme Court did not address the above-quoted conclusion of the Ninth Circuit.

But Defendants reading of *Verdugo-Urquidez* is off the mark. While the Court split on whether the Fourth Amendment applied to extraterritorial searches involving non-citizens, seven of the nine Justices expressly stated or implicitly agreed that the Warrant Clause did not apply to extraterritorial searches. Chief Justice Rehnquist, writing for the four-Justice plurality, specifically observed that an American warrant "would be a

dead letter outside the United States." *Verdugo-Urquidez,* 494 U.S. at 274. In his concurrence, Justice Kennedy similarly noted that the "absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country." *Id*. at 278 (Kennedy, J., concurring).

Since *Verdugo-Urquidez,* the Ninth Circuit has observed, "foreign searches have neither been historically subject to the warrant procedure, nor could they be as a practical matter." United States v. Barona, 56 F.3d 1087, 1093 n. 1 (9th Cir.1995). The Court agrees. First, as other courts have observed, there is no statutory basis for a magistrate judge in the Southern District of New York to issue a search warrant in a non-terrorism case targeting property even in the Eastern District of New York, let alone to issue such a warrant to be executed in London, England. Second, even if a magistrate judge took the view that he or she had such authority, as Detective Sergeant Shaw made quite clear, an American law enforcement officer would not be permitted under British law to waltz into a London premises and execute the search authorized by the American magistrate judge. Indeed, it takes little to imagine the diplomatic and legal complications that would arise if American government officials traveled to another sovereign country and attempted to carry out a search of any kind, professing the authority to do so based on an American-issued search warrant.

Even if the Warrant Clause does not apply to searches conducted by foreign governments, the question remains whether the Fourth Amendment's reasonableness requirement can limit the use of evidence seized by a foreign government from United States citizens. And, even if a foreign search must be reasonable, there is the question of whether there is a remedy in American courts for an unreasonable search. In answer to the latter question, the courts have consistently held that the exclusionary rule does not govern the conduct of foreign government officers. *See United States v. Janis*, 428 U.S. 433, 455 n. 31 (1976) ("It is well established, of course, that the exclusionary rule, as a deterrent sanction, is not applicable where a private party or a foreign government commits the offending act.").

However, the Second Circuit has recognized two exceptions to this rule. First, where the conduct of foreign officials in acquiring the evidence is 'so extreme that they shock the judicial conscience' a federal court in the exercise of its supervisory powers can require exclusion of the evidence so seized. Second, where cooperation with foreign law enforcement officials may implicate constitutional restrictions, evidence obtained by foreign officials may be excluded. Within the second category for excluding evidence, constitutional requirements may attach in two situations: (1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials.

There is no claim here, nor could there be, that the conduct of the Metropolitan Police officials "shocked the conscience." "Circumstances that will shock the conscience are limited to conduct that 'not only violates U.S. notions of due process, but also violates fundamental international norms of decency." ' United States v. Mitro, 880 F.2d 1480,

1483-84 (1st Cir.1989) (quoting Stephen A. Salzburg, *The Reach of the Bill of Rights Beyond the Terra Firma of the United States*, 20 Va. J. Int'l L. 741, 775 (1980)). Here, a Metropolitan Police officer sought the permission of . . . U.K. judicial officials to get a search warrant. This is conduct that soothes, rather than shocks, the conscience. Nor could there be a claim that the American Government's request for the Metropolitan Police to seek such a warrant was part of an effort to evade American legal restraints. As just noted, given the plain limits on the authority of American judicial officials to issue extraterritorial warrants, and given the limits on Postal Inspectors in unilaterally executing such warrants abroad, there was no basis for the Postal Inspectors here to think that they had any choice other than to make a treaty-based request for U.K. officials to carry out the search in London. Thus, the only question is whether the warrants which the Metropolitan Police officials executed are invalid.

The answer to this question, as it is with the legality of any search, depends on whether the search was reasonable. While the Second Circuit has not addressed this issue, other courts have held that a foreign search is reasonable if it meets the requirements of the law of the nation in which the search is executed, as long as those requirements do not permit conscious-shocking conduct. As such, Defendants' claims that the U.K. search was unreasonable under American standards because, for example, it was a general warrant that permitted seizure of virtually all Amerindo U.K. records or because it was not based on a finding of probable cause, are not dispositive. Indeed, Defendants cite to no authority to support this novel position.

As an alternative, Defendants spend a great deal of energy attempting to explain why the [U.K.] search contravened British law, but to no avail.[20] [Extensive discussion of English criminal procedure law omitted. The court concludes: "Applying these principles to this case, the Court rejects the claim by Defendants that the search of the Cadogan Tate facility violated U.K. law, or otherwise was unreasonable."]

Even if the U.K. search somehow contravened British law, however, suppression would be required only if it could be said that the Postal Inspectors could not reasonably and in good faith rely on the representations made to them by Detective Sergeant Shaw that the warrants were lawfully obtained. Where a foreign agent represents to an American official that their activity is lawful, and the American reasonably relies on it, the exclusionary rule does not serve its purpose as a deterrent. This is just an offshoot of the good-faith exception to the exclusionary rule recognized in *Leon*. In a typical extraterritorial search, as was the case here, American law enforcement officers are not in

---

[20] Each side elected to fight the battle over U.K. law with expert opinion. Defendants relied on a thoughtful "Report by English Counsel Instructed on Behalf of Mr. Tanaka." This report, prepared by English Barrister Clare Sibson, is a synopsis of U.K. law on searches. One obvious and admitted limitation of this report, however, is that Ms. Sibson had "not been made aware of the facts of the matter concerning Mr. Tanaka in New York." Therefore, among other things, Ms. Sibson offers no opinion about the legality of the warrants issued in connection with the Cadogan Tate search, nor does she say anything about the propriety of the statements Detective Sergeant Shaw made in support of the warrant applications. The Government countered by offering the testimony of Detective Sergeant Shaw. This testimony was helpful in the sense that it was based on the actual events of this case, but of course is limited by the fact that Detective Sergeant Shaw is neither a solicitor nor a barrister. That said, Detective Sergeant Shaw impressed the Court with his grasp of U.K. search and seizure law.

Though foreign law once was treated as an issue of fact, it now is viewed as a question of law and may be determined through the use of any relevant source, including expert testimony.

an advantageous position to judge whether the search was lawful, and holding them to a strict liability standard for failings of their foreign associates would be even more incongruous than holding them to a strict liability standard as to the adequacy of domestic warrants. Moreover, requiring American law enforcement officials to make extensive pre-search inquiries about the legality of a foreign government official's conduct would be diplomatically delicate, to say the least. Permitting reasonable reliance on representations about foreign law is a rational accommodation to the exigencies of foreign investigations.

The motions to suppress the evidence obtained in the United Kingdom search are denied.

.

CHAPTER 8:
JURISDICTION

On page 652, before the Notes and Questions, add the following:

On August 5, 2007, President Bush signed into law a significant amendment to FISA, the Protect America Act, Pub.L. 110-55, S. 1927. The Act clarifies that FISA warrants are not needed to monitor targets "reasonably believed to be located outside of the United States." The Act sets up a process by which the Executive branch determines a protocol for determining which communications belong to individuals located outside the United States and then submits the protocol to the judges of the FISA Court. The FISA Court must approve the protocol unless it finds clear error that the protocols are reasonably designed to identify the communications of individuals outside the United States and to collect their national security or terrorism related communications.

The Protect America Act has been the subject of significant debate since its passage in August 2007. Much of the reason is the ambiguity of the statute's terms. Critics suggest that the Act may be used to monitor the communications of those inside the United States by monitoring the international calls and e-mails of those inside the United States. Defenders of the Act contend that this is impossible because such monitoring would make those people targets of monitoring. They further argue that if someone inside the United States is actually sending or receiving information related to terrorism, the government would get a proper FISA warrant based on probable cause to be able to capture all of their communications.

Uncertainty over the meaning of the Protect America Act will likely lead to additional legislation within coming months. However, how the legislation is working in practice is difficult to know because the workings of national security terrorism investigations are classified.

On page 655 after Note 3, add:

4. For a detailed and sophisticated discussion of the law governing national security investigations, *see* David Kris & Doug Wilson, *National Security Investigations and Prosecutions* (West 2007).