FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant,* v. CHRISTOPHER LEE ADJANI; JANA REINHOLD, *Defendants-Appellees.*	No. 05-50092 D.C. No. CR-04-00199-TJH-01 OPINION

Appeal from the United States District Court
for the Central District of California
Terry J. Hatter, Chief District Judge, Presiding

Argued and Submitted
January 13, 2006—Pasadena, California

Filed July 11, 2006

Before: Mary M. Schroeder, Chief Judge,
Daniel M. Friedman* and Raymond C. Fisher,
Circuit Judges.

Opinion by Judge Fisher

*The Honorable Daniel M. Friedman, Senior United States Circuit Judge for the Federal Circuit, sitting by designation.

COUNSEL

Elyssa Getreu, Assistant United States Attorney, Los Angeles, California, for the plaintiff-appellant.

Marilyn E. Bednarski, Kaye, McLane & Bednarski, LLP, Pasadena, California, for defendant-appellee Jana Reinhold.

OPINION

FISHER, Circuit Judge:

While executing a search warrant at the home of defendant Christopher Adjani to obtain evidence of his alleged extortion, agents from the Federal Bureau of Investigation seized Adjani's computer and external storage devices, which were later searched at an FBI computer lab. They also seized and subsequently searched a computer belonging to defendant Jana Reinhold, who lived with Adjani, even though she had not at that point been identified as a suspect and was not named as a target in the warrant. Some of the emails found on Reinhold's computer chronicled conversations between her and Adjani that implicated her in the extortion plot. Relying in part on the incriminating emails, the government charged both Adjani and Reinhold with conspiring to commit extortion in violation of 18 U.S.C. § 371 and transmitting a threatening communication with intent to extort in violation of 18 U.S.C. § 875(d).

The defendants brought motions to suppress the emails, arguing that the warrant did not authorize the seizure and search of Reinhold's computer and its contents; but if it did,

the warrant was unconstitutionally overbroad or, alternatively, the emails fell outside the scope of the warrant. The district court granted the defendants' motion to suppress the email communications between Reinhold and Adjani, finding that the agents did not have sufficient probable cause to search Reinhold's computer, and that once they discovered information incriminating her, the agents should have obtained an additional search warrant. The government appeals this evidentiary ruling, but only with respect to three emails dated January 12, 2004.

The district court's ruling on the motion to suppress is subject to de novo review. *United States v. Vargas-Castillo*, 329 F.3d 715, 722 (9th Cir. 2003). We review de novo a district court's determination regarding the specificity of a warrant, including whether it is overbroad or not sufficiently particular. *United States v. Wong*, 334 F.3d 831, 836-37 (9th Cir. 2003). We hold that the government had probable cause to search Reinhold's computer, the warrant satisfied our test for specificity and the seized e-mail communications fell within the scope of the properly issued warrant.[1] Accordingly, we reverse the district court's order suppressing the January 12, 2004 email communications between Reinhold and Adjani.

I. Background

A. The Extortion Scheme[2]

[1]The FBI agents engaged in multiple searches and seizures here. First, FBI agents *searched* Adjani's residence. During the course of this search, the agents *seized* Reinhold's and Adjani's computers. Then, at the FBI computer lab, agents *searched* Reinhold's computer for evidence of the alleged extortion. Finally, the agents *seized* the three e-mails forming the basis of this appeal. For purposes of our analysis, however, we collapse the first three events into one, generally referring to it as the "search" of Reinhold's computer. As for the last event, we refer to it as the "seizure" of e-mail communications.

[2]The following factual summary is based entirely on the FBI affidavit presented to, and relied upon by, the magistrate judge in support of the FBI's request for an arrest warrant for Adjani and a search warrant for various premises.

Adjani was once employed by Paycom Billing Services Inc. (formerly Epoch), which facilitates payments from Internet users to its client websites. As a payment facilitator, Paycom receives and stores vast amounts of data containing credit card information. On January 8, 2004, a woman (later identified as Reinhold) delivered envelopes to three Paycom partners, Christopher Mallick, Clay Andrews and Joel Hall. Each envelope contained a letter from Adjani advising that he had purchased a copy of Paycom's database containing its clients' sensitive financial information. The letter threatened that Adjani would sell the Paycom database and master client control list if he did not receive $3 million. To prove his threats were real, Adjani included samples of the classified data. He directed the Paycom partners to sign an enclosed agreement attesting to the proposed quid pro quo and fax it back to him by January 12. The letter included Adjani's email address, *cadjani@mac.com*, and a fax number. Agents later learned that Adjani's email address was billed to Reinhold's account.

Evidence suggested that Adjani left Los Angeles on January 9, 2004, and ultimately ended up in Zurich, Switzerland. From Switzerland, Adjani sent an email on January 12 to Joel Hall to confirm that Hall and the others had received the envelopes. Adjani followed up on this email on January 13 by instructing Hall to contact him through AOL/Mac iChat instant messaging if he wanted to discuss the settlement agreement. With the FBI monitoring, Hall conversed several times with Adjani on the Internet and over the telephone. In spite of Adjani's insistence that he remain overseas, Hall convinced him to come to Los Angeles on January 26 to pick up $2.5 million in exchange for the database.

Adjani returned to Los Angeles on January 22, under FBI surveillance. Reinhold, driving in a car that the FBI had earlier identified as Adjani's, was observed leaving Adjani's residence in Venice, California, picking him up from the airport and returning to his residence. The FBI also observed Rein-

hold using an Apple computer, the same brand of computer Adjani used to email and chat with Paycom.

B. Obtaining and Executing the Search Warrant

On January 23, 2004, based on the facts recited above and attested to in FBI Agent Cloney's affidavit (which was affixed to the warrant), a federal magistrate judge granted the government an arrest warrant for Adjani and a search warrant covering Adjani's Venice residence, his vehicle, his person and the residence of the individual who had stolen the confidential information from Paycom. The warrant specifically sought "evidence of violations of [18 U.S.C. § 875(d)]: Transmitting Threatening Communications With Intent to Commit Extortion." Further, the warrant expressly authorized seizure of:

> 5g. Records, documents and materials containing Paycom's or Epoch's master client control documents, Paycom's or Epoch's email database, or other company information relating to Paycom or Epoch.
>
> 5h. Records, documents and materials which reflect communications with Christopher Mallick, Clay Andrews, Joel Hall or other employees or officers of Paycom or Epoch.
>
> 5i. Any and all evidence of travel, including hotel bills and receipts, gasoline receipts, plane tickets, bus tickets, train tickets, or any other documents related to travel from January 8, 2004 to the present.
>
> . . . .
>
> 5k. Computer, hard drives, computer disks, CD's, and other computer storage devices.

With respect to the computer search, the warrant prescribed the process to be followed: "In searching the data, the com-

puter personnel will examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein." Additionally, it noted that "[i]n order to search for data that is capable of being read or intercepted by a computer, law enforcement personnel will need to seize and search . . . . [a]ny computer equipment and storage device capable of being used to commit, further, or store evidence of the offense listed above."

On January 26, 2004, agents observed Reinhold driving Adjani, in a car registered to him, to his meeting with Paycom. While Adjani went into a hotel, Reinhold slipped into the backseat of his car, placing curtains over the windows. At this point, agents proceeded to search Adjani's car. That same day, agents executed the search warrant for Adjani's Venice residence. There they found and seized various computers and hard drives, including Reinhold's computer, which were later sent to an FBI computer lab to be searched. During that search process, the hard drive from Reinhold's computer revealed certain email correspondence between Reinhold and Adjani, implicating Reinhold in the extortion plot and supporting a charge of conspiracy against both of them.

The defendants successfully sought suppression of these seized email communications in the district court. This appeal requires us to determine whether the agents permissibly searched Reinhold's computer; whether the warrant satisfied our specificity standards; and whether the emails seized fell within the scope of the otherwise properly issued warrant.

II. Analysis

A. Probable Cause

The government principally argues that contrary to the district court's finding and the defendants' assertions, the search warrant affidavit established probable cause to search all

instrumentalities that might contain "evidence of violations of" 18 U.S.C. § 875(d), including Reinhold's computer and emails. Reinhold counters that the affidavit may have generally established probable cause, but did not do so with respect to *her* computer, because "[i]n the affidavit, Reinhold was not labeled as a target, suspect, or co-conspirator."

1. Probable cause to issue the warrant

[1] "A search warrant . . . is issued upon a showing of probable cause to believe that the legitimate object of a search is located in a particular place, and therefore safeguards an individual's interest in the privacy of his home and possessions against the unjustified intrusion of the police." *Steagald v. United States*, 451 U.S. 204, 213 (1981). As the Supreme Court has explained, the "probable cause standard . . . is a practical, nontechnical conception." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quoting *Brinegar v. United States*, 338 U.S. 160, 176 (1949)). Furthermore, "probable cause is a fluid concept — turning on the assessment of probabilities in particular factual contexts — not readily, or even usefully, reduced to a neat set of legal rules." *Id.* at 232; *see also United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc) ("Employing the principles of *Gates* — practicality, common sense, a fluid and nontechnical conception of probable cause, and deference to the magistrate's determination — we conclude that the search warrant was supported by probable cause.").

[2] The warrant here was supported by probable cause, because the affidavit submitted to the magistrate judge established that "there [was] a fair probability that contraband or evidence of a crime [would] be found in" computers at Adjani's residence.[3] *See Gates*, 462 U.S. at 238. The exten-

[3]Our conclusion that the agents could permissibly search Reinhold's computer does not rely upon the government's assertion that Adjani and Reinhold had "joint computers."

sive 24-page supporting affidavit described the extortion scheme in detail, including that Adjani possessed a computer-generated database and communicated with Paycom over email, requiring the use of a computer. *Cf. Gourde*, 440 F.3d at 1072 ("The details provided on the use of computers by child pornographers and the collector profile strengthen th[e] inference [that probable cause supported the warrant] and help 'provide[ ] context' for the 'fair probability' that Gourde received or downloaded images." (internal citation omitted)). Furthermore, the agent's affidavit explained the need to search computers, in particular, for evidence of the extortion scheme: "I know that considerable planning is typically performed to construct and consummate an extortion. The plan can be documented in the form of a simple written note or more elaborate information stored on computer equipment."

[3] "Probable cause exists if 'it would be reasonable to seek the evidence in the place indicated in the affidavit.' " *United States v. Wong*, 334 F.3d 831, 836 (9th Cir. 2003) (quoting *United States v. Peacock*, 761 F.2d 1313, 1315 (9th Cir. 1985)). The crime contemplated by the warrant was *transmitting* a threatening communication with intent to extort. *See* 18 U.S.C. § 875(d). To find evidence of extortion, the government would have probable cause to search for and seize instrumentalities likely to have been used to facilitate the transmission. The magistrate judge could rightfully assume that there was a "fair probability" that such evidence could be contained on computers or storage devices found in Adjani's residence.

2. Probable cause to search "Reinhold's computer"

[4] Having held that the affidavit supporting the warrant established probable cause to search for and seize instrumentalities of the extortion (including records, files and computers) in Adjani's residence, we turn to Reinhold's contention that the probable cause for the Adjani warrant did not extend so far as to permit a search of her property. We disagree. The

agents, acting pursuant to a valid warrant to look for evidence of a computer-based crime, searched computers found in Adjani's residence and to which he had apparent access. That one of the computers actually belonged to Reinhold did not exempt it from being searched, especially given her association with Adjani and participation (however potentially innocuous) in some of his activities as documented in the agent's supporting affidavit.[4] The officers therefore did not act unreasonably in searching Reinhold's computer as a source of the evidence targeted by the warrant. *See Illinois v. Rodriguez*, 497 U.S. 177, 185 (1990) (holding Fourth Amendment requires officers to act *reasonably* in executing a search warrant); *Brinegar v. United States*, 338 U.S. 160, 176 (1949).

Reinhold's argument that there was no probable cause to search her computer, a private and personal piece of property, because the warrant failed to list her as a "target, suspect, or co-conspirator" misunderstands Fourth Amendment jurisprudence.[5] Although individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers, we have never held that agents may establish probable cause to search only those items owned or possessed by the criminal suspect. The law is to the contrary. "The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is

[4]The affidavit expressly referred to Reinhold multiple times, including that: (1) Reinhold delivered the envelopes containing the threat to Paycom partners; (2) after leaving his house and driving his car, Reinhold picked Adjani up from the airport upon his return from Switzerland; and (3) Adjani's email address (*cadjani@mac.com*) was billed to Reinhold.

[5]The district court appears to have agreed with Reinhold's argument when it noted that "[t]here's not probable cause of any kind mentioned in the search warrant itself to deal with any property of Ms. Reinhold." However, as we explain below, probable cause analysis focuses not on the owner of the property, but rather on whether evidence of the crime can be found on the property given the circumstances.

sought." *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978); *cf. United States v. Ross*, 456 U.S. 798, 820-21 (1982) ("A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search.").

[5] In *United States v. Hay*, 231 F.3d 630 (9th Cir. 2000), the defendant made an argument similar to Reinhold's, challenging the district court's ruling allowing evidence of child pornography found on his computer to be used against him at trial. Hay claimed that the affidavit submitted by officers to obtain a warrant did not establish probable cause to engage in a search of Hay's computer because "there was no evidence that he fell within a class of persons likely to collect and traffic in child pornography because the affidavit does not indicate that he was a child molester, pedophile, or collector of child pornography and sets forth no evidence that he solicited, sold or transmitted child pornography." *Id.* at 635. We rejected Hay's challenge, holding that "[i]t is well established that a location can be searched for evidence of a crime even if there is no probable cause to arrest the person at the location." *Id.* (citing *Zurcher*, 436 U.S. at 556). *See also United States v. Taketa*, 923 F.2d 665, 674 (9th Cir. 1991) ("[T]he correct inquiry is whether there was reasonable cause to believe that evidence of . . . misconduct was located on the property that was searched."); *United States v. Tehfe*, 722 F.2d 1114, 1118 (3d Cir. 1983) ("Property owned by a person absolutely innocent of any wrongdoing may nevertheless be searched under a valid warrant."); *United States v. Melvin*, 596 F.2d 492, 496 (1st Cir. 1979) (holding the *Zurcher* rule applies to "a person who the police do indeed suspect but do not have probable cause to arrest; such a person's property may be searched upon probable cause to believe that fruits, instrumentalities, or evidence of the crime are present, even though the products of the search may implicate him.").

[6] Likewise, there was no need here for the agents expressly to claim in the affidavit that they wanted to arrest Reinhold, or even that Reinhold was suspected of any criminal activity. The government needed only to satisfy the magistrate judge that there was probable cause to believe that evidence of the crime in question — here extortion — could be found on computers accessible to Adjani in his home, including — as it developed — Reinhold's computer.[6] By setting forth the details of the extortion scheme and the instrumentalities of the crime, augmented by descriptions of Reinhold's involvement with Adjani, the government satisfied its burden. The magistrate judge therefore properly approved the warrant, which in turn encompassed all the computers found at Adjani's residence.

B. Specificity Requirement

The defendants argue that if the warrant did authorize a search that properly included Reinhold's computer, the warrant was fatally overbroad, justifying the district court's exclusion of the Reinhold emails. The government counters that the warrant satisfied the particularity standards articulated by this court, so exclusion was improper.

[7] The Fourth Amendment's specificity requirement prevents officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized. *See United States v. McClintock*, 748 F.2d 1278, 1282 (9th Cir. 1984) ("[G]eneral warrants are prohibited." (internal quotation marks omitted)); *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982) ("Nothing is left to the discretion of the officer executing the warrant." (internal quotation marks and citation omitted)). However, the level of detail necessary in a warrant

[6]The warrant signed by the magistrate judge plainly authorized a search of all computers, hard drives, computer disks and other computer storage devices in the Adjani residence.

is related to the particular circumstances and the nature of the evidence sought. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). "Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Id.*

In determining whether a warrant is sufficiently particular, we consider one or more of the following factors:

> (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.

Id. at 963 (internal citations omitted).

Spilotro involved a warrant issued against individuals suspected of loan sharking and gambling activities. *See id.* at 960. The warrant authorized "the seizure of address books, notebooks, notes, documents, records, assets, photographs, and other items and paraphernalia evidencing violations of the multiple criminal statutes listed." *Id.* at 964. It failed, however, to state the "precise identity, type, or contents of the records sought." *Id.* Partly because of this reason, we held that the warrant was not sufficiently specific to pass muster under the Fourth Amendment. More could have been done to tie the documents sought to the crimes alleged by, for example, stating that the police were searching for "records relating to loan sharking and gambling, including pay and collection sheets, lists of loan customers, loan accounts and telephone numbers . . . ." *Id.* (internal quotation marks and citation omitted).

[8] In contrast to *Spilotro*, the warrant to search Adjani's residence satisfied our specificity criteria. First, we have

already held that there was probable cause to search the computers. As to the second factor, the warrant objectively described the items to be searched and seized with adequate specificity and sufficiently restricted the discretion of agents executing the search. The warrant affidavit began by limiting the search for evidence of a specific crime — transmitting threatening communications with intent to commit extortion. *See id.* ("Reference to a specific illegal activity can, in appropriate cases, provide substantive guidance for the officer's exercise of discretion in executing the warrant."); *see also United States v. Wong*, 334 F.3d 831, 837-38 (9th Cir. 2003) ("The specificity of the items listed in the warrant combined with the language . . . directing officers to 'obtain data as it relates to this case' from the computers is sufficiently specific to focus the officer's search."); *Cardwell*, 680 F.2d at 76-77 (holding impermissibly general a warrant where "the only limitation on the search and seizure of appellants' business papers was the requirement that they be the instrumentality or evidence of violation of the general tax evasion statute," but noting that if the warrant is cabined by a "preambulatory statement limiting the search to evidence of particular criminal episodes," it may fulfill the particularity requirement). Further, unlike in *Spilotro*, the Adjani warrant provided the "precise identity" and nature of the items to be seized. *Spilotro*, 800 F.2d at 964. For example, paragraph 5h of the warrant instructed agents to search for documents reflecting communications with three individuals or other employees of a specific company. Also, paragraph 5i authorized seizure of "any" evidence of travel but provided a specific, though not exhaustive, list of possible documents that fell within this category and temporally restricted the breadth of the search. *Cf. United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980) (cited favorably in *Cardwell*, 680 F.2d at 77-78) (holding a warrant was not sufficiently particular because "[t]he officers' discretion was unfettered, there is no limitation as to time and there is no description as to what specific records are to be seized."). Moreover, the extensive statement of probable

cause in the affidavit detailed the alleged crime and Adjani's unlawful scheme. *See Spilotro*, 800 F.2d at 964 (considering favorably warrants "describing the criminal activit[y] . . . rather than simply referring to the statute believed to have been violated.").

[9] With respect to the final *Spilotro* factor, we conclude that the government described the items to be searched and seized as particularly as could be reasonably expected given the nature of the crime and the evidence it then possessed. The Adjani warrant "describe[d] in great[ ] detail the items one commonly expects to find on premises used for the criminal activities in question. . . ." *Spilotro*, 800 F.2d at 964; *see also United States v. Mann*, 389 F.3d 869, 877 (9th Cir. 2004) ("While a search warrant must describe items to be seized with particularity sufficient to prevent a general, exploratory rummaging in a person's belongings, it need only be reasonably specific, rather than elaborately detailed.") (internal quotation marks and citation omitted).

Center Art Galleries-Hawaii, Inc. v. United States, 875 F.2d 747 (9th Cir. 1989), the principal case defendants rely upon in making their overbreadth argument, is distinguishable. In that case, we held that a warrant providing for "the almost unrestricted seizure of items which are 'evidence of violations of federal criminal law' without describing the specific crimes suspected is constitutionally inadequate." *Id.* at 750 (quoting *Spilotro*, 800 F.2d at 964). In contrast, the government here did describe at some length both the nature of and the means of committing the crime. Further, unlike in *Center Art Galleries*, the affidavit was expressly incorporated into the warrant. *Id.* ("An affidavit can cure the overbreadth of a warrant if the affidavit is 'attached to and incorporated by reference in' the warrant.") (quoting *Spilotro*, 800 F.2d at 967, and citing *United States v. Leary*, 846 F.2d 592, 603 (10th Cir. 1988)).[7]

[7]The supporting affidavit attached to the warrant set forth a detailed computer search protocol, including instructions as to when the computers

We understand the heightened specificity concerns in the computer context, given the vast amount of data they can store. As the defendants urge, the warrant arguably might have provided for a "less invasive search of Adjani's [email] 'inbox' and 'outbox' for the addressees specifically cited in the warrant, as opposed to the wholesale search of the contents of all emails purportedly looking for evidence 'reflecting' communications with those individuals." Avoiding that kind of specificity and limitation was not unreasonable under the circumstances here, however. To require such a pinpointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought. *Cf. Ross*, 456 U.S. at 821 ("When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand."). Moreover, agents are limited by the longstanding principle that a duly issued warrant, even one with a thorough affidavit, may not be used to engage in a general, exploratory search. *See*

---

should be searched on-site rather than taken off-site and procedures for screening the data to determine what data could be searched and seized under the terms of the warrant. *See also* U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 43, 69 (July 2002) (detailing what FBI agents should include in warrants when they contemplate the need to search computers). Such specificity increases our confidence that the magistrate judge was well aware of what he was authorizing and that the agents knew the bounds of their authority in executing the search. *Cf. Hay*, 231 F.3d at 636 (considering favorably an affidavit providing "that searches and seizures of evidence from computers requires agents to seize all parts of a computer system to be processed later by a qualified computer expert.").

The protocol, of course, does not eliminate the necessity that the protocol procedures and the materials seized or searched fall within the scope of a properly issued warrant supported by probable cause.

United States v. Rettig, 589 F.2d 418, 423 (9th Cir. 1978) ("Where evidence is uncovered during a search pursuant to a warrant, the threshold question must be whether the search was confined to the warrant's terms. . . . [T]he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed. It must not be a general exploratory search . . . ." (internal quotation marks and alterations omitted)); *see also Franklin v. Foxworth*, 31 F.3d 873, 875 (9th Cir. 1994) ("[T]he reasonableness of a search or seizure depends not only on *when* it is made, but also on *how* it is carried out." (internal quotation marks omitted and emphasis in original)).

Computer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of Adjani's (or Reinhold's) labeling of the files documenting Adjani's criminal activity. The government should not be required to trust the suspect's self-labeling when executing a warrant. *See Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) ("Defendants may legitimately have checked to see that the contents of the directories corresponded to the labels placed on the directories. Suspects would otherwise be able to shield evidence from a search simply by 'misfiling' it in a directory labeled 'e-mail.' "); *cf. United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("[A]ll items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.").

C. Scope of the Warrant

Even assuming that the warrant was supported by probable cause and was adequately specific such that a search of Reinhold's computer and emails were permissible, Reinhold argues that the actual emails sought to be introduced into evi-

dence were outside the scope of the warrant. Again, we disagree.

[10] The three seized emails the government seeks to admit clearly fall within the scope of paragraph 5h of the warrant affidavit, authorizing seizure of "[r]ecords, documents and materials which reflect communications with Christopher Mallick, Clay Andrews, Joel Hall or other employees or officers of Paycom or Epoch," which are relevant evidence of violations of 18 U.S.C. § 875(d). Each email specifically refers to communication with Joel Hall or one of the stated companies (identifying them by name).[8] Reinhold's argument that the term "reflect communications with" should be read narrowly to cover only those emails sent between one of the named Paycom employees and Adjani is nonsensical. The government already had the emails sent between the victims of the extortion and Adjani — obtained from the victims themselves. The purpose of the warrant was to obtain further and corroborating evidence of the extortion scheme and Adjani's criminal intent in communicating with the victims, and the three emails plainly "reflect" the relevant communications specified in paragraph 5h.

To the extent Reinhold argues that the emails were outside the scope of the warrant because they implicated her in the crime and supported a charge of conspiracy to commit extortion (a crime not specifically mentioned in the warrant), we reject the argument. There is no rule, and Reinhold points to no case law suggesting otherwise, that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evi-

[8]The first email, sent from Adjani to Reinhold, states, in relevant part, "I sent Joel the message." The second, a reply from Reinhold, states, "I thought that you were going to wait until after today if they don't respond to send Joel an email?" The third, another email from Reinhold to Adjani, states, "I assume you have read Joel's fax by now. Funny or sucky thing is that I had ran out the door just 3 minutes before he sent that to go to a payphone to call Epoch . . . . A girl answered and I asked for Joel Hall."

dence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant.

[11] In *United States v. Beusch*, 596 F.2d 871 (9th Cir. 1979), the defendants argued that certain seized items, including two ledgers and a file, should be excluded because they contained information unrelated to the suspect identified in the warrant. The defendants claimed that the officers impermissibly engaged in a general search by not segregating out those items implicating a third individual in the crime. We rejected this proposition and refused to impose the burden of segregation on the police. In so doing we held,

> All three items admittedly contained information seizable under the terms of the warrant and they therefore met the particularity requirement of the Fourth Amendment. As long as an item appears, at the time of the search, to contain evidence reasonably related to the purposes of the search, there is no reason absent some other Fourth Amendment violation to suppress it. The fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part. In so holding we are careful to point out that we are discussing single files and single ledgers, i.e., single items which, though theoretically separable, in fact constitute one volume or file folder.

Id. at 877 (internal citation omitted). *Beusch* is analogous to the situation at hand. The agents were rightfully searching Reinhold's computer for evidence of Adjani's crime of extortion. They were looking in Reinhold's email program when they came across information that was both related to the purposes of their search and implicated Reinhold in the crime. That the evidence could now support a new charge against a new (but already identified) person does not compel its suppression. On these facts, we disagree with the district court's

conclusion that the officers should have obtained a new search warrant when they came across the incriminating emails. In so concluding, we are careful to note that in this case the evidence discovered was clearly related to the crime referred to in the warrant. We need not decide to what extent the government would be able to introduce evidence discovered that the police knew, at the time of discovery, was not related to the crime cited in the warrant. *Cf. United States v. Carey*, 172 F.3d 1268, 1272-73 (10th Cir. 1999) (excluding certain evidence of child pornography where the warrant authorized only seizure of drug evidence and the detective knew he was expanding the scope of the warrant, and holding that the officer should have stopped the search and obtained a new warrant.).

III. Conclusion

"The Fourth Amendment incorporates a great many specific protections against unreasonable searches and seizures." *Beusch*, 596 F.2d at 876-77. The contours of these protections in the context of computer searches pose difficult questions. Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be protected, the latter discovered.[9] As society grows ever more reliant on computers as a

[9]The fear that agents searching a computer may come across such personal information cannot alone serve as the basis for excluding evidence of criminal acts. As the Supreme Court has noted in a different context:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a war-

means of storing data and communicating, courts will be called upon to analyze novel legal issues and develop new rules within our well established Fourth Amendment jurisprudence. *See* Eric L. Probst and Kerri A. Wright, *Using Their E-Words Against Them*, NEW JERSEY LAW JOURNAL, Jan. 30, 2006, at S1 (noting that tens of billions of emails are sent daily). The fact of an increasingly technological world is not lost upon us as we consider the proper balance to strike between protecting an individual's right to privacy and ensuring that the government is able to prosecute suspected criminals effectively. In this era of rapid change, we are mindful of Justice Brandeis's worry in *Olmstead v. United States*,

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?

277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

We do not now have occasion to address the myriad complex issues raised in deciding when a court should exclude evidence found on a computer, but are satisfied that the agents in this case acted properly in searching Reinhold's computer and seizing the emails in question here. The district court erred in excluding these emails. Therefore, the district court's

---

> rant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

ruling on the motion to suppress is reversed, and this matter is remanded for further proceedings consistent with this opinion.

REVERSED and REMANDED.