UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CRIMINAL NO. 06-10082-RGS

UNITED STATES OF AMERICA

v.

KENDRA D'ANDREA and
WILLIE JORDAN

MEMORANDUM AND ORDER ON DEFENDANTS' MOTIONS TO SUPPRESS

July 20, 2007

STEARNS, D.J.

BACKGROUND

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.[1] The caller reported that Jane Doe,[2] 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 (90 Veteran's Way in Gloucester,

[1]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.

[2]I will refer to the child by the pseudonym "Jane Doe."

Massachusetts), the log-in name and password for the website, and the number of a cellular telephone used by defendants.

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.[3] The warrant was executed shortly after midnight. The searching officers found D'Andrea, two young children (including Jane Doe), and a mobile camera telephone.[4] 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.[5]

---

[3]The affidavit submitted by Detective Fitzgerald in support of the warrant application exhibits a high degree of computer sophistication.

[4]The camera phone was searched pursuant to separate state and federal warrants authorizing the examination of its contents. It was found to contain a number of sexually explicit pictures of Jane Doe. There is no merit in defendants' argument that the seizure of the camera phone was unauthorized. The warrant permitted the seizure of "cameras" and "computer storage devices." The modern cellular telephone fits easily into these categories. It can also be a "computer accessory," as the warrant also specified.

[5]Jordan was arrested in Michigan and returned to Massachusetts on a warrant obtained by the Gloucester police. At the time of his arrest, police seized Jordan's personal cell phone. There is no indication in the record that a search of its contents yielded anything of an incriminating nature.

D'Andrea and Jordan now move to suppress the downloaded images,[6] the evidence seized from 90 Veteran's Way, and any incriminating statements made by D'Andrea and Jordan.[7] Defendants allege that Curley (the DSS supervisor) violated their Fourth Amendment rights by accessing the Sprint PCS website and downloading the images.[8] 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.[9] Wong Sun v. United States, 371 U.S. 471, 487-488 (1963). Defendants also seek a hearing pursuant

[6]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.

[7]It is not clear from the record that Jordan in fact made any incriminating admissions.

[8]As part of the federal investigation, agents obtained warrants a year later for the Sprint PCS account records, as well as for records associated with defendants' cell phones.

[9]The court denied defendants' request for an evidentiary hearing after determining on the basis of defendants' submissions and oral argument that a hearing was unnecessary. The purpose of such a hearing, as defendants defined it, would have been to establish the reasonableness of their expectation of privacy in the website. As will be seen from the analysis, the granting of such an expectation has no bearing on the outcome of the motion. There is no requirement that an evidentiary hearing be held where a defendant has failed to "allege facts 'sufficiently definite, specific, detailed and non-conjectural, to enable the court to conclude that a substantial claim is presented.'" United States v. Migely, 596 F.2d 511, 513 (1st Cir. 1979), quoting Cohen v. United States, 378 F.2d 751, 761 (9th Cir. 1967).

to Delaware v. Franks, 438 U.S. 154 (1978), to challenge the veracity of Detective Fitzgerald's search warrant affidavit.[10]

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? See Rakas v. Illinois, 439 U.S. 128, 143-144 n.12 (1978). The reasonableness of an asserted interest in privacy is determined by the totality of the circumstances.

> Thus, the Court has examined whether a person . . . took normal precautions to maintain his privacy. . . . Similarly, the Court has looked to the way a person has used a location, to determine whether the Fourth Amendment should protect his expectations of privacy. . . . The Court on occasion also has looked to history to discern whether certain types of government intrusion were perceived to be objectionable by the Framers. . . . And, as the Court states today, property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas[.]

Id. at 152-153. 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

[10]Defendants allege that there is a material inconsistency between Fitzgerald's warrant affidavit and a Secret Service agent's report summarizing a DSS supervisor's account of what she had been told by the hotline worker. The Fitzgerald affidavit states that DSS had received a tip that Jane Doe was the victim of sexual abuse that "was occurring at 90 Veteran's Way." According to defendants, the agent's report does not quote the DSS supervisor as saying that the hotline monitor had been told by the tipster of D'Andrea's address. The (no longer) anonymous caller told an investigator for the defendants that when she made the report to DSS, she did not know where D'Andrea lived.

astonishing if it were not – the question still remains whether this expectation is one that society would recognize as reasonable.

In many areas of human interaction, Fourth Amendment privacy claims are deemed *per se* unreasonable. For example, there can be no reasonable expectation of privacy in matters voluntarily disclosed or entrusted to third parties, even those disclosed to a person with whom one has a confidential business relationship.[11] See Smith v. Maryland, 442 U.S. 735, 744-745 (1979) (no reasonable expectation of privacy on the part of a phone subscriber in numbers dialed through telephone company switching equipment). See also United States v. Payner, 447 U.S. 727, 731-732 (1980) (no reasonable expectation of privacy in information contained in records entrusted to a bank officer); United States v. Miller, 425 U.S. 435, 442-443 (1976) (same, customer's bank records); United States v. White, 401 U.S. 745, 750 (1971) (same, confidences exchanged in private conversation with others).

The Smith line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access.[12] See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (a user loses any

---

[11]I recognize that some State courts have come to a different conclusion interpreting their own State Constitutions. See, e.g., State v. Reid, 914 A.2d 310 (N.J. Super. Ct. App. Div. 2007). While it is not determinative, the Massachusetts Supreme Judicial Court is not among them. See Commonwealth v. Vinnie, 428 Mass. 161, 178 (1998) (no expectation of privacy in dialed telephone numbers); Commonwealth v. Cote, 407 Mass. 827, 834-835 (1990) (same, messages forwarded through a telephone answering service).

[12]A URL (Uniform Resource Locator) is the commonly used textual designation of the address of an Internet website. The URL is used to locate the specific web server that

expectation of privacy in personal subscription information when it is conveyed to a system operator); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D. N.Y. 2002) (criminal defendants have no Fourth Amendment privacy interest in subscriber information supplied to an internet service provider). Cf. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) ("[I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect the information."). See also United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of [the Electronic Communications Privacy Act]."), aff'd, 106 Fed. Appx. 688 (10th Cir. 2004); United States v. Hambrick, 55 F. Supp. 2d 504, 509 (W.D. Va. 1999) (same), aff'd, 225 F.3d 656 (4th Cir. 2000).

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

---

hosts the site. See In re Pharmatrak, Inc., 329 F.3d 9, 13 n.2 (1st Cir. 2003). When a user types in a particular URL, the user's computer queries an interconnected set of global databases known as the domain name system (DNS) to locate the Internet Protocol (IP) address of the host web server. The contacted DNS server first checks its own database, and if it cannot find the URL address, queries other DNS servers for "the unique address assigned to every machine on the Internet." Id. at 13 n.1. A web host offers a customer the ability to post a website or web page to the world wide web. A web hosting company may provide a single website for a large customer, or it may host multiple websites for multiple customers. See Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606, 617 (E.D. Pa. 2004). A virtual web host (like Sprint PCS) typically maintains a single web server with a single IP address on which it hosts multiple on-line communities as sub-pages of its primary domain name. The "sub-pages or sub-domains are usually independent of the provider and independent of each other." Id.

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, even though each form of protection is penetrable."[13] LaFave, 1 Search and Seizure § 2.6 at 721 (4th ed. 2006). Professor LaFave's argument is persuasively echoed in Warshak v. United States, 2007 WL 1730094 (6th Cir. June 18, 2007).

> [T]he 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 [v. United States, 389 U.S. 347 (1967)], 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.
>
> . . .

[13]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).

> 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." [Smith,] 442 U.S. at 43. 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 it has been granted access.

Id. at *10-11 (emphasis in original).

The protections of the Fourth Amendment, it must be emphasized, apply only to the actions of the State and its agents. Burdeau v. McDowell, 256 U.S. 465, 475 (1921). 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. See Coolidge v. New Hampshire, 403 U.S. 443, 489-490 (1971) (wife voluntarily gave her husband's guns and clothing to police); United States v. Mekjian, 505 F.2d 1320, 1326-1327 (5th Cir. 1975) (osteopath's secretary secretly photocopied his fraudulent Medicare billings and mailed them to the FBI); United States v. Pryba, 502 F.2d 391, 400-401 (D.C. Cir. 1974) (a curious freight agent opened a package and turned its pornographic contents over to the FBI); United States v. Feffer, 831 F.2d 734, 737-738 (7th Cir. 1987) (a disgruntled employee supplied authorities with documents implicating her supervisor in a crime); Ward v. State, 351 A.2d 452, 454-455 (Md. Ct. Spec. App. 1976) (daughter gave police a tape cassette implicating

her father in a murder). See also United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003) (a vigilante computer hacker provided authorities with digital images of the defendant engaging in sexual activity with a child).

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.[14] 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.[15] 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.[16] 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

---

[14]Nor would the State be responsible for the caller's acts even had she hacked her way into the defendants' website (instead of obtaining the password from one of the defendants).

[15]There is no dispute that for purposes of the state action requirement, Curley was a state actor. See Commonwealth v. Howard, 446 Mass. 563, 569 (2006); Dubbs v. Head Start, Inc., 336 F.3d 1194, 1205 (10th Cir. 2003).

[16]A website, like a computer file, is properly analogized to a file cabinet or other physical containers in which records can be stored.

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). See Paul v. State, 57 P.3d 698, 702-703 (Alaska Ct. App. 2002) (police did not intrude on any Fourth Amendment expectation of privacy by reviewing the entirety of an obscene videotape that had been partially viewed by a private citizen).

At day's end, this case falls clearly into the "assumption of the risk" exception identified in Warshak and Supreme Court precedent.[17] "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. See also United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) (the sender of an email runs the risk that its recipient will publish its contents). 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.[18]

---

[17]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.

[18]The government's "emergency intervention" argument, based on Brigham City, Utah v. Stuart, U.S. , 126 S.Ct. 1943 (2006), among other cases, provides a sufficient alternative basis on which to uphold the search of D'Andrea's apartment. See also United States v. Bradley, 321 F.3d 1212, 1214-1215 (9th Cir. 2003); Laney v. State, 117 S.W.3d 854, 862-863 (Tex. Crim. App. 2003) (en banc). DSS had received powerful evidence that

THE FRANKS HEARING REQUEST

While a judicial ruling on a motion to suppress is ordinarily confined to the "four corners" of the affidavit, there are circumstances in which a defendant may challenge the truthfulness of statements made by an applicant for a search warrant. See Franks v. Delaware, 438 U.S. 154, 156 (1978). Cf. United States v. Southard, 700 F.2d 1, 7 (1st Cir. 1983) (a facially sufficient affidavit is entitled to a presumption of validity). To be entitled to a Franks hearing, a defendant must make a "substantial preliminary showing" that an affidavit submitted in support of a warrant application contains intentionally false or recklessly untrue statements that are material to a finding of probable cause. Franks, 438 U.S. at 155-156.

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

Id. at 171.

Defendants' request for a Franks hearing is flawed by two fundamental errors, one legal, and the other factual. A Franks hearing is addressed to the veracity and care of the

---

a young child was being sexually abused and that images of that abuse were being disseminated on the internet. It would have been a dereliction of duty for it to fail to act. While not directly relevant to the facts of this case, the ECPA contains an emergency provision permitting an ISP provider to disclose account information to a governmental entity "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure . . . ." 18 U.S.C. § 2702(c)(4).

affiant. Id. at 171. The credibility of an informant is tested not by Franks. It is tested by the rules of Gates.[19] See United States v. Carmichael, 489 F.2d 983, 989 (7th Cir. 1973). Defendants' argument is that DSS, in reporting the anonymous caller's information to Detective Fitzgerald, embellished the information by including the Veteran Way's address and the allegation that the abuse was taking place in D'Andrea's apartment. Even were this so – the evidence is overwhelmingly to the contrary – Detective Fitzgerald would have had no reason to question the reliability of DSS or the basis of its information regarding the abuse of Jane Doe. See United States v. Ventresca, 380 U.S. 102, 110-111 (1965); United States v. Del Toro Soto, 676 F.2d 13, 19-20 (1st Cir. 1982). Stated differently, the issue is not whether DSS gave Detective Fitzgerald false or misleading information, but whether Fitzgerald as the affiant fabricated or misrepresented what he had been told by DSS. See United States v. Jones, 208 F.3d 603, 607 (7th Cir. 2000); Lawmaster v. United States, 993 F.2d 773, 775 (10th Cir. 1993). There is no evidence – certainly no "substantial showing" – that he did.

The defendants' factual error is more straightforward. They state that a summary of the hotline monitor's account of the anonymous call provided by a DSS supervisor to a Secret Service agent does not make any reference to D'Andrea's apartment. Putting aside the layers of hearsay contained in the agent's report, an original copy of the DSS Intake Information Form, which was provided to the court under seal, makes it plain that the caller did give the hotline monitor D'Andrea's address. Moreover, defendants misstate what the

[19] Illinois v. Gates, 462 U.S. 213 (1983). See also Aguilar v. Texas, 378 U.S. 108 (1964); Spinelli v. United States, 393 U.S. 410 (1969).

agent wrote in his report. His summary begins with a reference to an anonymous caller reporting that a child was being sexually abused "at the D'Andrea residence."

ORDER

For the foregoing reasons, the motion to suppress physical evidence is DENIED. The motion to suppress D'Andrea's statements is DENIED. The motion for an evidentiary hearing is DENIED. The motion for a Franks hearing is DENIED. The Clerk will set the case for trial.[20]

SO ORDERED.

/s/ Richard G. Stearns

_____

UNITED STATES DISTRICT JUDGE

[20]Because the case raises issues of legal (although not factual complexity), the government's motion to exclude the time taken by the court to render its decision will be allowed. The government will file a proposed Speedy Trial Act Order to that effect within seven (7) days.