IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA v. LAURENCE JOHN BODE	Criminal Case No. ELH-12-158

MEMORANDUM OPINION

Defendant Laurence John Bode is charged by Indictment (ECF 1) with five counts of child pornography offenses, in violation of 18 U.S.C. § 2252(a)(2) and (a)(4).[1] The charges stem from the government's investigation of the users of Free6.com, a website that hosted legal adult pornography and sexual content and also provided an online instant messaging or "chat" functionality. The investigation was spawned by a federal agent's suspicion that some of Free6.com's users were exchanging child pornography by way of the website's chat service.

During the investigation, Free6.com's administrator gave the agent administrative access privileges to the website, which included the ability to view the content of chat messages sent between individual users of the website. In the chat messages, the agent observed two alleged images of child pornography, among other things, which had been transmitted by a user in January 2010. Further investigation provided probable cause to believe that this user was Mr. Bode or a member of his household. On this basis, the government obtained a search warrant for Mr. Bode's home and computers. The search of the defendant's home was conducted on

[1] In particular, defendant is charged with two counts of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) (Counts One and Two, alleging conduct on or about January 21 and 26, 2010, respectively); two counts of receipt of child pornography, in violation of the same statute (Counts Three and Four, alleging conduct on or about February 8, 2010, and June 2, 2010, respectively); and a single count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4) (Count Five).

October 8, 2010, pursuant to a warrant. At that time, Bode's computer was seized, and a subsequent forensic examination of the computer revealed additional digital files containing alleged child pornography.

Following his indictment in March 2012, Bode filed several pretrial motions.[2] At issue here is Bode's Motion to Suppress Tangible and Derivative Evidence ("Motion") (ECF 32), in which Bode argues that the agent's perusal of the chat messages on Free6.com constituted an unlawful search or seizure, in violation of the Fourth Amendment; the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*; and/or the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* Thus, defendant maintains that all of the evidence derived in the government's investigation is tainted by the unlawful search and should be suppressed.

The Motion has been fully briefed, and evidence and argument were presented on it at a hearing on May 7 and 8, 2013.[3] Three witnesses testified at the hearing: Special Agents Neil Burdick and John Van Wie, both of the Department of Homeland Security, and Nicola Thyen, defendant's spouse. Transcripts of the testimony have since been prepared. *See* Tr. of 5/7/13

[2] In addition to the Motion at issue here (ECF 32), Bode filed a Motion to Suppress Statements (ECF 16) and a Motion for a Hearing Pursuant to *Franks v. Delaware* ("*Franks* Motion") (ECF 34), concerning the application for the search warrant. These motions were also heard on May 7 and 8, 2013. As I memorialized in an Order of May 9, 2013 (ECF 65), for reasons stated on the record at the hearing, I denied both the Motion to Suppress Statements and the *Franks* Motion, but I reserved ruling as to certain issues reflected in those motions that were dependent on the outcome of the present Motion (ECF 32).

[3] In resolving the Motion (ECF 32), I have considered the supporting Memorandum (ECF 33); the government's Opposition (ECF 43); defendant's Reply (ECF 47); the government's Surreply (ECF 57), filed with leave of court, *see* ECF 59, and post-hearing memoranda submitted by both sides. *See* Bode Post-Hearing Memo (ECF 66); Gov't Post-Hearing Memo (ECF 67). In addition, I have considered exhibits filed by the parties with their briefing and the testimony and exhibits presented at the hearing.

(ECF 94); Tr. of 5/8/13 (ECF 95).[4] For the reasons that follow, I will deny the Motion.

Factual Summary

I find the following facts, derived from the evidence submitted at the hearing, as well as the undisputed portions of the parties' submissions. *See United States v. Castellanos*, 716 F.3d 828, 847 (4th Cir. 2013) (stating that "'any . . . fact at a suppression hearing' must be 'established only by a preponderance of the evidence'") (quoting *United States v. Helms*, 703 F.2d 759, 763-64 (4th Cir. 1983).

A. Free6.com

In 2008, Special Agent Neil Burdick of the Department of Homeland Security, assigned to Immigration and Customs Enforcement, attended the 2008 Internet Crimes Against Children Conference, where he was informed that the chat service on Free6.com was used by some users of the website to download and distribute child pornography. Accordingly, in late September or early October of 2008, SA Burdick began to investigate the website from his office in California, where he was part of the Child Exploitation Investigations Group.

In order to utilize Free6.com's chat service at that time, a visitor to the website had to click an icon labeled "chat" on the main Free6.com home page. This would take the user to a page titled "Chat log in," where the user was prompted to fill out a form asking the user to choose a screen name and to indicate the user's gender, and then to click a button labeled "Log In." The following text appeared to the right of the login form:

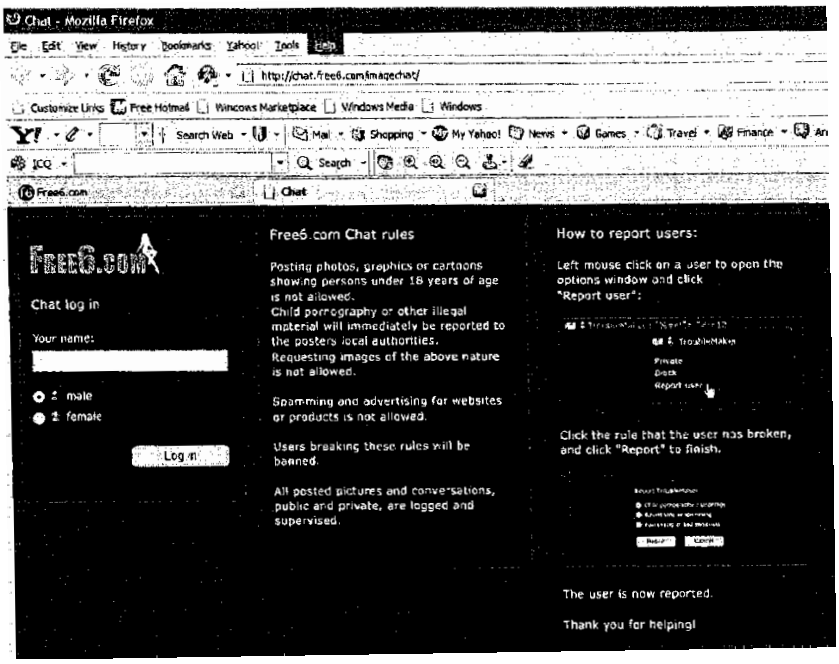
[4] The testimony of Agent Van Wie and Ms. Thyen was relevant only to the Motion to Suppress Statements and the *Franks* Motion. Accordingly, I have not recounted it.

> Free6.com Chat rules
>
> Posting photos, graphics or cartoons showing persons under 18 years of age is not allowed.
> Child pornography or other illegal material will immediately be reported to the posters [sic] local authorities. Requesting images of the above nature is not allowed.
>
> Spamming and advertising for websites or products is not allowed.
>
> Users breaking these rules will be banned.
>
> All posted pictures and conversations, public and private, are logged and supervised.

The parties refer to the text of the "Free6.com Chat rules," quoted above, as a "banner." To the right of this "banner" were instructions for "How to report users," which gave users of the chat service the option to report other users who violated the rules. The instructions indicated that the reporting user would have three options to indicate the nature of the infringing content that an offending user had posted: (1) "Child pornography / underage"; (2) "Advertising or spamming"; or (3) "Harassing or bad behavior."

An image of this page of the Free6.com website, as it appeared when SA Burdick began his investigation, is shown below.[5]

[5] The images showing the appearance of various sections of the Free6.com website are taken from exhibits submitted by the parties. They were authenticated by the testimony of SA Burdick, who also described the functionality of the website. There is no apparent dispute that the images are true and accurate depictions of the website as it appeared at the relevant times.



Notably, although the login page asked the user for "Your Name," Free6.com did not require users to enter their true identity or to register in any way with the website. Rather, the user would enter a screen name, which might—or might not—represent the user's true identity. Moreover, the screen name was not tied to a permanent account; it was only valid for the user's current chat session, and there was no password requirement. So, a user could use a different screen name each time he or she logged into the chat service on the website.

In any event, once a user clicked on the "Log In" button, the user would be presented with the user interface for the chat service. However, before the user could actually use the chat service, the user was required to click a button labeled "ACCEPT," to indicate acceptance of the contents of a second "banner" that appeared above the user interface. At the time SA Burdick began his investigation, the second banner contained a non-pornographic image of a young girl staring sadly into the camera, and the following text:

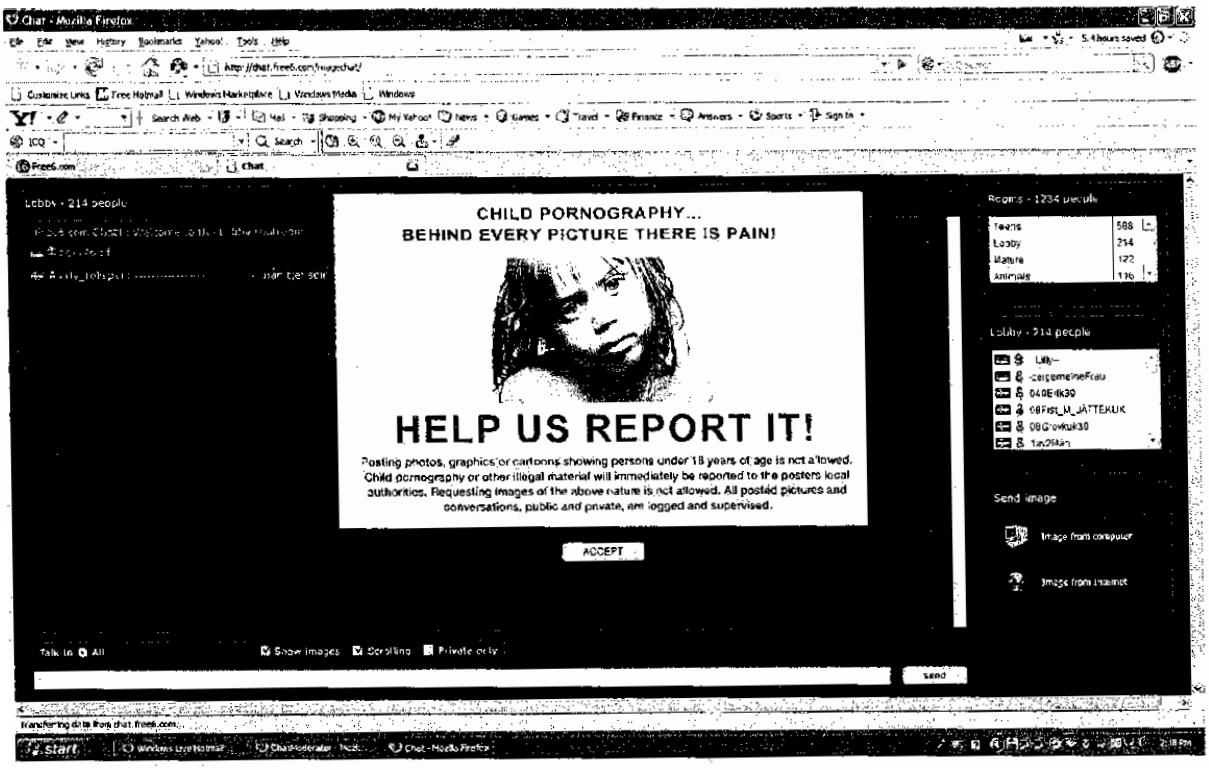
CHILD PORNOGRAPHY…

BEHIND EVERY PICTURE THERE IS PAIN!

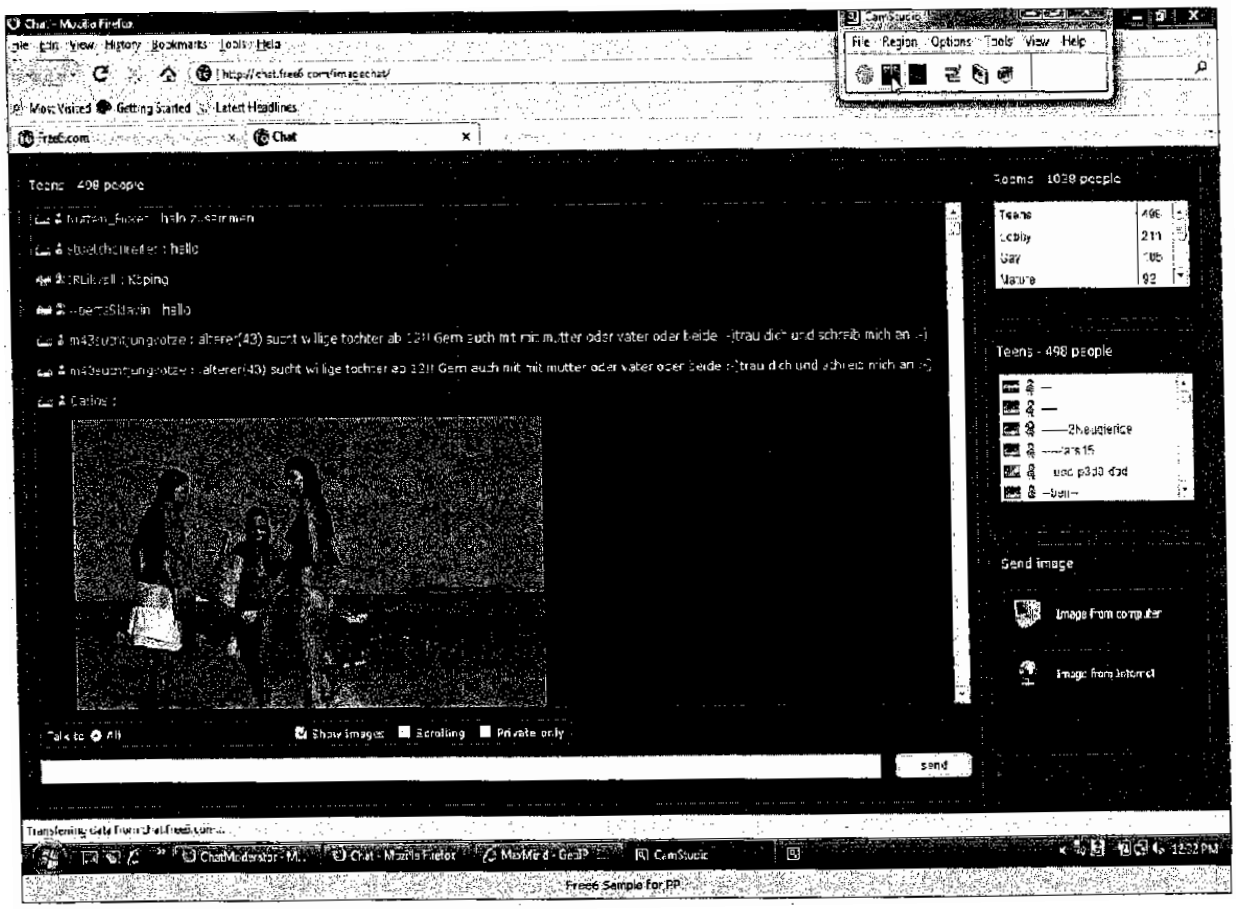
HELP US REPORT IT!

Posting photos, graphics or cartoons showing persons under 18 years of age is not allowed. Child pornography or other illegal material will immediately be reported to the posters [sic] local authorities. Requesting images of the above nature is not allowed. All posted pictures and conversations, public and private, are logged and supervised.

An image of the user interface of the Free6.com chat service, including the second banner superimposed over it, is shown below.



Once a user clicked the "ACCEPT" button, he or she would be able to use the chat service. An image demonstrating the user interface for the chat service is shown below.



The chat service allowed users to send real-time messages, consisting of text or images, to virtual "chat rooms," in which any number of users—members of the public—might be present, as well as to send "private" chat messages directly to individual users. In essence, the chat service functioned as a web-based instant messaging service. Unlike an email account, an online bulletin board, or the comments section of a blog, there was no way for a user in a public chat room to see messages that had been posted when the user was not logged in. Nor could a user in a public or private chat room access messages he or she sent or received during a previous session.

According to SA Burdick, he personally observed several people using the chat service on Free6.com to post child pornography. Tr. of 5/7/13 at 4. This prompted Burdick to contact the website's administrator. *Id.* SA Burdick initially served a subpoena on a company called Domains by Proxy in order to obtain the identity and contact information for the owner or administrator of Free6.com. *Id.* at 5-6.[6] Based on the response to the subpoena, SA Burdick learned that Free6.com was "run in Sweden." *Id.* at 7. Therefore, SA Burdick did not send a

[6] Apparently, Free6.com was a customer of Domains by Proxy and, when SA Burdick attempted to learn the identity of Free6.com's owner, he received only Domains by Proxy's information. The evidence did not describe the specific role played by Domains by Proxy. But, the company describes itself on its website as a "Whois privacy service." *See* http://www.domainsbyproxy.com/ (last visited Aug. 16, 2013). *Cf. Jeandron v. Bd. of Regents of Univ. Sys. of Md.*, 510 F. App'x 223, 227 (4th Cir. 2013) ("A court may take judicial notice of information publicly announced on a party's web site, so long as the web site's authenticity is not in dispute and 'it is capable of accurate and ready determination.'") (quoting Fed. R. Evid. 201(b) and citing *O'Toole v. Northrop Grumman Corp.*, 499 F.3d 1218, 1225 (10th Cir. 2007)).

To understand the role of Domains by Proxy, it is helpful to provide some background information regarding the Internet's domain name registration system. Websites are typically accessed by a "domain name," *e.g.*, "google.com," or "Free6.com." "A domain name is 'any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.'" *Barcelona.com, Inc. v. Exelentisimo Ayuntamiento de Barcelona*, 330 F.3d 617, 623 (4th Cir. 2003) (citation omitted). "To obtain a domain name, a would-be registrant simply makes application to a registrar ([in 2003,] there [were] over 160), submits a fee, and agrees to the terms of the domain name registration agreement. Domain names are assigned on a first-come, first-served basis." *Id.* at 623-24. Domain name registrars contribute registration information to "WHOIS," "a publically available online database" that is "compiled by registrars from information submitted by registrants," through which "users can access information regarding domains, including the registrant's name, address, phone number, and e-mail address." *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1064 n.22 (9th Cir. 2009).

Domains by Proxy acts as an agent for website owners, by listing its own name and contact information (rather than the actual website owner's) in the WHOIS database entry for a given domain name. *See generally* http://www.domainsbyproxy.com/ (last visited Aug. 16, 2013). Then, Domains by Proxy forwards to the website owner communications that are intended for the owner, and promises its customers that it will not reveal their identity and contact information, except as required by law (*e.g.*, in response to a valid subpoena) or in other defined circumstances. *See id.*

subpoena to Free6.com, because "they're a foreign company and [he had] no authority to send a subpoena to a company in Sweden." *Id.* Rather, he "[d]ecided it would be easier to e-mail them and see if they would cooperate." *Id.*

Accordingly, on October 6, 2008, SA Burdick sent an email to the administrator of Free6.com (via an anonymous email address provided by Domains by Proxy). He wrote, ECF 33-3 at 1:

> I am looking for contact information for the person who monitors the chat portion of your website for child pornography. Your website claims that it reports child sexual abuse images to authorities. I have seen numerous postings of child pornography and would like to receive reports about the people in the United States who are doing this. I have no interest in investigating your website, only the people in the United States that are posting these images.

A few days later, Free6.com's administrator, who identified himself to Burdick only as "Stefan,"[7] responded via email, stating, ECF 33-3 at 3:

> Thanks for your e-mail.
>
> What we can do for you is to provide you with a log in and password to our administrator area. In there you will be able to search by username and see every post that user has made in the chat (including "private" messages and pictures) also time and IP number of the users will be available.
>
> I will get back to you in a day or two with login details. Please feel free to contact me again if there is anything else that we can do to assist you. We are as much against child pornography as you are and will be happy to assist.

SA Burdick replied: "That would be absolutely fantastic! I thank you for your willingness to help and look forward to working with you." ECF 33-3 at 5. On October 24,

[7] SA Burdick subsequently learned that Stefan's full name is Stefan Sederholm. Sometime after February 2010, Burdick learned that Sederholm had been arrested in the Philippines in April 2009 in connection with alleged sex offenses. *Id.* at 41-44. According to news accounts cited by defendant, Sederholm was convicted in May 2011 of sex trafficking crimes in the Philippines, and he is now serving a life sentence in that country.

2008, Stefan sent an email to Burdick containing the address of the private administrative website for the chat service of Free6.com, and Burdick's own username ("neilburdick") and password to access the administrative website. ECF 33-3 at 9. Burdick replied: "I really can't thank you enough for helping me with this." ECF 33-3 at 11.

SA Burdick proceeded to investigate the users of Free6.com by means of his access to the chat messages that he could then peruse via his administrative access to the website. Indeed, the investigation of Free6.com consumed much of Burdick's time between October 24, 2008, and late February 2010, when the website was shut down. *See* Tr. of 5/7/13 at 19.[8] One feature of the administrative website for the chat service was that an administrator could select a particular user, either by screen name or IP address,[9] and see a log of that user's sent messages (including messages sent in public chat rooms as well as messages sent in "private" chats with other individual users), over a period of recent time.[10] Although this feature displayed a log of

[8] SA Burdick testified that in late February 2010, after the salient events in this case, Free6.com was shut down. Burdick testified credibly that his task force did not shut the website down. Rather, he first learned of the situation when he attempted to access the website and found that it was no longer functional. *See* Tr. of 5/7/13 at 41.

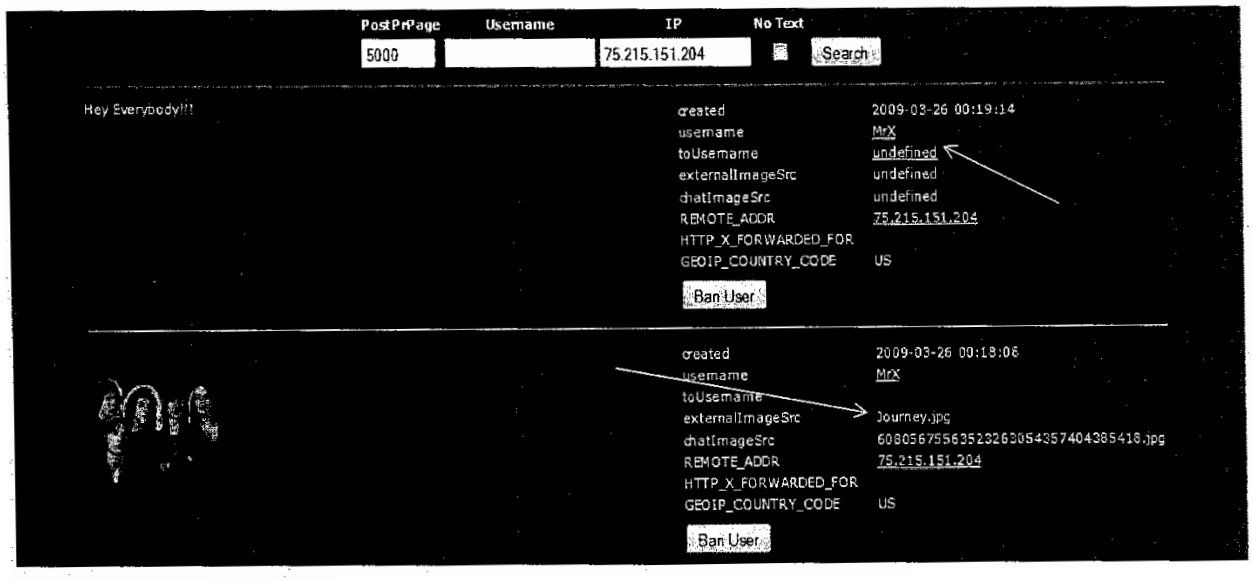
[9] "IP" is the abbreviation for "Internet Protocol." Each computer or other device "connected to the Internet is assigned a unique numerical address, otherwise known as an Internet protocol or IP address, to identify itself and facilitate the orderly flow of electronic traffic." *Peterson v. Nat'l Telecommc'ns & Info. Admin.*, 478 F.3d 626, 629 (4th Cir. 2007). "IP addresses are usually written as four decimal numbers separated by dots (periods)," where "each of the four numbers is in the range 0-255," for example: 192.168.0.1. Craig Hunt, TCP/IP NETWORK ADMINISTRATION § 2.2 (O'Reilly 3d ed., 2002).

[10] When the chat messages connected with defendant were sent, the website was logging each user's sent chat messages for the previous six or seven days. Messages that were older than the logging period were automatically deleted, a measure which SA Burdick presumed was for the purpose of saving storage space on the computers hosting the website. *See* Tr. of 5/7/13 at 11.

SA Burdick believed that when he gained administrative access, the logging period was six or seven days. *See id.* at 14. He was challenged on this point by defense counsel, who

messages sent by the selected user, it did not show messages received by the selected user.

An image showing an example of the log for a particular user (selected by IP address) is shown below.



For each chat message, the log showed, on the left side of the screen, the text or the image that had been posted. On the right side of the screen, the log showed several items of information about the chat message, including the following:

---

directed his attention to an ICE "Report of Investigation" ("ROI") dated February 27, 2009, authored by Burdick, *see* ECF 33-2, which stated: "Among the items readily available to administrators are: all chats a person has had on the website *within a 24 hour period*, [and] all pictures posted by that person *within a 24 hour period*[.]" *Id.* at 4 (emphasis added). SA Burdick conceded that the logging period "may have . . . started as 24 [hours]" and have been later increased by Free6.com's administrators to six or seven days. Tr. of 5/7/13 at 14. However, he did not remember asking Free6.com's administrators to increase the logging period. *Id.* at 14-15.

There is no need to resolve whether the logging period was increased at SA Burdick's request, as the defense suggests. Even if it was, this would be legally relevant only to the question of whether Free6.com was acting as a government agent at the relevant times. And, as discussed *infra*, the government has conceded, for purposes of the Motion, that Free6.com was acting as its agent within the meaning of relevant Fourth Amendment doctrine.

- "created": The date and time (in Boston, Massachusetts, where the actual computer servers hosting the Free6.com website were located) that the chat message was sent. *See* Tr. of 5/7/13 at 56.

- "username": The screen name of the user who sent the message.

- "toUsername": The screen name of the user to whom the message was sent. If the chat message was not sent privately to an individual user, but was sent instead to a public chat room, the "toUsername" field would be blank, or would contain the value "null" or "undefined." *See* Tr. of 5/7/13 at 26.

- "externalImgSrc": If the chat message consisted of an image, the filename of the image file as sent by the user. (If the chat message consisted of text, this field was "undefined.")

- "REMOTE_ADDR": The IP address of the user who sent the chat message.

- "GEOIP_COUNTRY_CODE": The country from which the user had sent the chat message, to the extent that the country could be discerned from the IP address.

As shown, each listing of a chat message in the log also included a button labeled "Ban User."

In his Motion, defendant contends that the message logging function of the administrative website allowed SA Burdick to intercept chat messages in real time. Upon consideration of the evidence, I do not find that the logging function was a real-time interception method. Rather, as SA Burdick credibly testified, each chat message sent by a user was transmitted to Free6.com's web server, where it was transmitted to the chat room or individual user to whom it was directed, while a copy of the message was stored in the log on the Free6.com server. Thus, any administrator (including Burdick) who viewed a user's chat log was viewing stored copies of the user's chat messages. *See* Tr. of 5/7/13 at 18-19. To be sure, although SA Burdick testified that he did not know how much "lag time" there was between when a message was sent via the chat service and when it appeared in the log, there is no reason to believe that any appreciable amount

of time would elapse. Thus, it may well be that the logging feature could be used to accomplish the practical equivalent of real-time interception, by simply refreshing the log repeatedly every few moments for newly logged messages.

I need not contemplate the legal implications of using the chat log as a *de facto* means of real-time interception, however, because SA Burdick testified credibly that, at least in connection with the messages that are connected to Mr. Bode, he did not use the log in that manner. Rather, SA Burdick testified that, although he occasionally would "look at the live web site and [see] that maybe someone was posting some questionable material" and then might "search by their IP address or by their nickname" for other potentially illegal content, the "vast majority" of his investigation utilized the "banned user" function of the administrative website.

As noted, the chat service included a mechanism for a user to report another user for violating the "Free6.com Chat rules," and provided users with instructions, on the login page for the chat service, as to how to report an offending user. SA Burdick testified that, if a user reported another user for violating the rules, this would have the effect of adding the user to a list of "banned users" that was accessible within the administrative website, so that the Free6.com administrators could view the log of the offending user's messages and determine whether it was appropriate to ban the user from accessing the website. *See* Tr. of 5/7/13 at 13, 58.[11]

According to SA Burdick, he regularly reviewed the message logs for users who had

[11] Based on SA Burdick's description of the "banned users" function, it appears that "banned users" was something of a misnomer, because the listing of "banned users" was not a list of users who had already been banned, but rather was a list of users who had been reported for potential banning. In any event, the evidence does not disclose what technical means were used to accomplish "banning" a user, but the precise nature of those means is not relevant to the matters at issue. SA Burdick testified that he personally banned a user on only one occasion, who was located in the United Kingdom. Therefore, SA Burdick did not pursue further investigation of that user. *See* Tr. of 5/7/13 at 59.

been newly added to the list of banned users to determine whether the users had transmitted child pornography. Although SA Burdick had no specific recollection of investigating the user who would later be identified with Mr. Bode, *see* Tr. of 5/7/13 at 21, I conclude, for reasons explained *infra*, that SA Burdick did not discover the messages at issue here via *de facto* real-time monitoring. It appears that SA Burdick reviewed the banned user list to discover the messages at issue here.

When SA Burdick initially obtained administrative access to Free6.com, he did not consult with government attorneys regarding the appropriateness or legality of using his administrative access to investigate users of the website. *See* Tr. of 5/7/13 at 10. However, in early 2009, SA Burdick realized that the investigation of Free6.com was likely to generate "a lot of spinoff cases," and so he consulted with counsel in the United States Attorney's Office in Los Angeles about the investigation. *See id.* at 30. An Assistant U.S. Attorney in that office advised Burdick that the two "banners" on the website (*i.e.*, the "Free6.com Chat rules" and the banner with the girl's image and the admonition to "HELP US REPORT" child pornography) might not be sufficient to cause users of the website to "relinquish[ ] their expectation of privacy" in their chat messages. *Id.* at 30-31.

SA Burdick testified that he suspended his monitoring of Free6.com between January 6, 2009, and February 13, 2009. Tr. of 5/7/13 at 37. Moreover, he indicated that the United States Attorney's office declined to use in prosecutions any messages gleaned from the beginning of his investigation until February 13, 2009, except for two instances in which there was "a child in imminent danger." *Id.* at 34-35.

In response to the concern expressed by the United States Attorney's office, SA Burdick again contacted Stefan, the administrator of Free6.com, to request an addition to the language of one of the banners. Specifically, in an email sent to Stefan on February 12, 2009, ECF 33-6 at 1, Burdick wrote:

> I wanted to keep you updated as to the progress of our investigation so far and discuss one further issue with you. To date, we have identified roughly 25 users in the United States of the Free6.com chat portion that have been trading child pornography on a regular basis.
>
> Your help and cooperation with this has been absolutely invaluable and I really can't tell you how grateful I am that you and your company are willing to help! Unfortunately however, we have run into a slight problem going forward with the investigation due to a loophole in American laws regarding the Internet. The attorneys working on this case have asked me to ask you if you would consider adding one line to the warning banners that users must go through in order to access the chat portion of your website. They have told me that if you add the line "Free6 may disclose these communications to the authorities at its discretion," following the statement reading "All posted pictures are logged and supervised, etc." that we will be able to legally view the administrator's section you have provided me access to.
>
> I realize this is a great deal to ask, and I really hate asking you to make these changes. I will also say that if it is possible to do so, it will lead to the eradication of a good portion of the illegal activity taking place on your website.
>
> I again thank you for your cooperation . . . .

Shortly thereafter, on or about February 13, 2009, Free6.com's administrator's made the requested change to the language of the second banner. After February 13, 2009, SA Burdick resumed reviewing messages on the website nearly every day. *Id.* at 38. On February 26, 2009, Stefan replied to Burdick by email, stating: "Sorry for the late response, but your text has been online for some time now. Please check if it's ok, and let me know if there is anything else we can do to help your investigation." ECF 33-6 at 2. Burdick responded: "The addition to the warning banner is absolutely perfect! Again, I can't thank you enough for your help . . . ." *Id.*

According to SA Burdick, *see* Tr. of 5/7/13 at 37 & 62, from on or about February 13, 2009, until Free6.com was ultimately shut down in February 2010—including the period of time in January 2010, when the messages at issue in this case were sent—the second warning banner on the site contained the added language, "Free6 may disclose these communications to the authorities at its discretion," such that the banner, in its entirety, stated:

> CHILD PORNOGRAPHY…
>
> BEHIND EVERY PICTURE THERE IS PAIN!
>
> HELP US REPORT IT!
>
> Posting photos, graphics or cartoons showing persons under 18 years of age is not allowed. Child pornography or other illegal material will immediately be reported to the posters [sic] local authorities. Requesting images of the above nature is not allowed. All posted pictures and conversations, public and private, are logged and supervised. **Free6 may disclose these communications to the authorities at its discretion.**

(Bold emphasis added to show added language.) As noted, each time a user of the Free6.com chat service logged into the chat service, he or she had to click a button labeled "ACCEPT" below this banner in order to use the chat service.

B. The Messages at Issue

On January 26, 2009, at approximately 4:19 p.m. in California (7:19 p.m. in Massachusetts, where the servers housing the Free6.com website were located), SA Burdick used the Firefox web browser to save a copy of the message log for a particular user of the chat service, identified by the IP address 173.13.192.238 (hereafter, the "Target Address"). *See* Tr. of 5/7/13 at 56-60; *see also* ECF 33-9 (log of chats from Target Address). When he testified on May 7, 2013, SA Burdick had no independent recollection of his investigatory actions on January 26, 2009. *See* Tr. of 5/7/13 at 21. However, he testified on the basis of a record of the

date and time that he had created the file containing the copy of the Target Address's message log, and his memory of his ordinary and customary practices at that time. *See id.* at 60.

As noted, SA Burdick testified that the "vast majority" of his investigation utilized the "banned users" function of the administrative website. *Id.* at 24. Although Burdick did not recall viewing the log associated with the Target Address on January 26, 2009, he testified that he believed he had accessed the Target Address's log from the banned user list, in accordance with his usual practice, *see id.* at 58, and the times associated with the messages at issue support that conclusion (or, at least, support the conclusion that SA Burdick did not monitor the communications from the Target Address in real time). The earliest chat message contained in the Target Address's log was sent on January 19, 2010 at 8:02:43 a.m., Eastern Standard Time. *See* ECF 33-9 at 77. The latest message contained in the log was sent on January 26, 2010, at 9:11:25 a.m., Eastern Standard Time (when it would have been 6:11 a.m. in California, where SA Burdick was located). As noted, SA Burdick testified that the file in which he saved the contents of the log was created at 4:19 p.m. Pacific Standard Time, approximately ten hours after the last message contained in the log was sent. Accordingly, I conclude, based on the preponderance of the evidence, that SA Burdick did not view the log of the Target Address's messages in real time or any practical approximation of real time.

Some messages in the log were sent to public chat rooms, but others were sent as private messages to other individual users. Although all of the messages contained in the log originated from the Target Address, they were sent using a variety of usernames. Initially, from 8:02 a.m. until 8:39 a.m. on January 19, 2010, the messages were sent under the username "DadsHome." Then, on the same date, from 9:59 a.m. until 10:28 a.m., the username "Mr4Play" was used. The

next day, January 20, 2010, from 6:46 a.m. until 11:45 a.m., the user of the Target Address posted using the username "DadonCam." The following day, January 21, 2010, the user utilized the name "DadsHere," from 7:40 a.m. until 10:59 a.m., when the user switched to the username "Kim26Asian."

Notably, when posting as "DadsHome," "Mr4Play," and "DadsHere," the user repeatedly posted (among other things) a non-pornographic photograph, purportedly of himself. *See* Gov't Motion Hearing Exh. 3. Based on my having seen Mr. Bode in court at the hearing, it appears to be a photograph of Mr. Bode. On a number of occasions, the user also identified himself as "Larry," indicated that he was typing from "Maryland" or the "Beaches in Maryland," stated that he "live[d] on [the] water," and provided the email address "larry_loans@[ ]."[12] In addition, the user stated that he was the father of two teenaged girls, and posted non-pornographic pictures of two girls who supposedly were his daughters. In fact, the defense has indicated that Mr. Bode has no children.

When the user switched to the username "Kim26Asian," the user repeatedly posted, among other things, several non-pornographic (but provocatively posed) images of a young woman of Asian descent, apparently to impersonate that woman. The user posted as "Kim26Asian" until 11:12 a.m. on January 21, 2010, and posted a handful of messages using the same username at about 1:24 p.m. on January 24, 2010.

On January 25, 2010, the user again began posting under the username "DadonCam," beginning at 7:46 a.m. and continuing until 9:15 a.m. The next day, January 26, 2010, the user posted as "DadonCam" from 7:02 a.m. until 7:17 a.m. About two hours later, at about 9:11 a.m.,

[12] I have redacted the email address for privacy reasons.

the user posted three messages using the username "DadsHome," which are the last messages contained in the log.

Many of the messages that the user sent were images, and most of the images that the user sent have not been provided to the Court. However, the government's application for the search warrant for the defendant's residence, obtained during the investigation of Mr. Bode, relied, in significant part, on two particular image files containing alleged child pornography that were included in the log of messages sent by the user from the Target Address.[13] The first image has the filename "~2spa102.jpg" and was sent ten times during the period covered by the log, invariably as a private message to another individual user of the chat service. The "~2spa102.jpg" image file actually consists of two separate pictures displayed side by side. The picture on the right shows a woman, seated, with her torso bare and her left breast exposed. A naked, prepubescent girl, approximately 8-10 years old in appearance, is seated on the right side of the woman's lap. The girl's legs are spread open and her vagina is exposed. The picture on the right shows the same woman and girl standing, clothed only in socks and shoes. The girl is using her hands to squeeze both of the woman's breasts.

The other image file upon which the warrant application relied has the file name "-11 radator.jpg." Unlike the "~2spa102.jpg" file, the "-11 radator.jpg" file was posted exclusively to public chat rooms in the chat service, on thirteen occasions during the period covered by the log. The "-11 radator.jpg" file consists of an image of two naked minor females,

[13] Printed copies of the image files were provided to the Court for review pursuant to 18 U.S.C. § 3509(m), and were returned to the custody of the government at the hearing on May 8, 2013.

one standing behind the other. Each girl is touching the other's pelvic area, and both are facing the camera.

C. The Investigation

Further investigation revealed that the Target Address was assigned to Comcast, an internet service provider. In April 2010, the government sent a subpoena to Comcast requesting subscriber records related to the Target Address during the period from January 19, 2010, at 8:02 a.m. EST to January 26, 2010, at 9:11 a.m. EST (*i.e.*, the time period covered by the log). Comcast responded with several items of information, including that the subscriber of the Target Address was Larry Bode; the service address in Ocean City, Maryland;[14] and that the IP address of the account was statically assigned, meaning that the Target Address was reserved for Mr. Bode's account, rather than having a different IP address assigned to the account each time the user accessed the internet. *See* ECF 33-11.

On October 5, 2010, the government submitted an application to then-Magistrate Judge James K. Bredar of this Court[15] for a search warrant for Mr. Bode's residence in Ocean City, Maryland, on the basis of the facts reviewed *supra*, as well as other information developed during the investigation. Judge Bredar issued the warrant, concluding that the evidence presented by the government established probable cause to search defendant's residence and, among other things, any computers found there. The search warrant was executed on October 8, 2010. A computer was seized from the residence, and a forensic examination of the computer revealed additional images and videos of alleged child pornography, as well as further evidence

[14] For the purpose of this opinion, it is not necessary to provide the particular street address.

[15] Judge Bredar is now a District Judge.

connecting Mr. Bode to the messages that had been posted via the Free6.com chat service. During the search, Mr. Bode was interviewed by investigators and gave statements that were the subject of his Motion to Suppress Statements (ECF 16). *See* note 2, *supra*.

Discussion

Defendant urges suppression of all of the government's evidence, on the ground that the evidence was derived from the Target Address's logged chat messages via the Free6.com chat service and, according to Bode, SA Burdick's review of those messages violated the Fourth Amendment, the Wiretap Act, and/or the Stored Communications Act. Accordingly, I begin by setting out some basic principles applicable to those constitutional and statutory provisions.

The Fourth Amendment guarantees, *inter alia*, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court stated that "the Fourth Amendment protects people, not places," *id.* at 351, and formulated a test for when a "search" within the meaning of the Fourth Amendment has occurred. Under the *Katz* standard, a search occurs when officers of the government invade a person's "reasonable expectation of privacy," a concept that imposes "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 260-61 (Harlan, J., concurring).[16] Ordinarily, "[w]hen there is

[16] Although the "reasonable expectation of privacy" test was formulated in Justice Harlan's concurrence in *Katz*, rather than the majority opinion, the Supreme Court's "later cases have applied the analysis of Justice Harlan's concurrence" as the operative standard. *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945, 950 (2012). In the recent *Jones* decision, however, the Supreme Court stated that "Fourth Amendment rights do not rise or fall with the *Katz* formulation," *id.*, and that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, [a] common-law trespassory test," *id.* at 952 (emphasis in original), whereby

no reasonable expectation of privacy, the Fourth Amendment is not implicated." *United States v. Davis*, 690 F.3d 226, 241 (4th Cir. 2012) (petition for cert. pending).

Moreover, even if a search or seizure occurs, the Fourth Amendment "does not proscribe all [government]-initiated searches and seizures; it merely proscribes those which are unreasonable." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991); *see Whren v. United States*, 517 U.S. 806, 809-10 (1996); *Illinois v. Rodriguez*, 497 U.S. 177, 183 (1990); *United States v. Sharpe*, 470 U.S. 675, 682 (1985); *United States v. Mendenhall*, 446 U.S. 544, 551 (1980). To be sure, warrantless searches "are *per se* unreasonable under the Fourth Amendment—subject to only a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357. To the extent that SA Burdick's perusal of the Target Address's message log constituted a search, it was conducted without a warrant. However, "valid consent to seize and search items provides an exception to the usual warrant requirement." *United States v. Buckner*, 473 F.3d 551, 554 (4th Cir.) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973)), *cert. denied*, 550 U.S. 913 (2007). The relevant Fourth Amendment doctrines are discussed in more depth, *infra*.

---

the government performs a search when it "physically occupie[s] private property for the purpose of obtaining information." *Id.* at 949. In addition, five concurring justices in *Jones* seemed to endorse the proposition that "long term monitoring" of a person's activities (even activities conducted in public) "impinges on expectations of privacy" and could constitute a search under the Fourth Amendment. *Id.* at 964 (Alito, J., concurring in judgment); *see also id.* at 955 (Sotomayor, J. concurring) (joining majority opinion but also endorsing standard articulated by Justice Alito).

Nevertheless, the parties have advanced arguments only under the reasonable expectation of privacy standard articulated in *Katz* and its progeny. Moreover, the facts in this case are not analogous to those in *Jones*, which involved extensive monitoring of a vehicle's location by means of a global positioning system (GPS). Accordingly, I need not consider the trespass standard discussed by the *Jones* majority or potential extensions of the reasonable expectation of privacy standard forecast by the *Jones* concurrences.

Defendant also relies on the Wiretap Act and the Stored Communications Act, two pieces of legislation that are closely interrelated. The Wiretap Act, now codified at 18 U.S.C. §§ 2510 *et seq.*, was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), "in response to considerable social and political activity on a variety of fronts." Clifford S. Fishman & Anne T. McKenna, 1 WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:10, at 1-16 (3d ed. 2012) ("WIRETAPPING"). In particular, as the Senate Judiciary Committee Report on the legislation reflects, in the forty years of case law and statutory development between the Supreme Court's decision in *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (holding that "wire tapping . . . did not amount to a search or seizure within the meaning of the Fourth Amendment"), and its 1967 decision in *Katz*, *supra*, 389 U.S. at 352-53 (holding that "a person in a telephone booth may rely upon the protection of the Fourth Amendment," and stating: "we have since departed from the narrow view on which [*Olmstead*] rested"), leading up to enactment of the Wiretap Act, the "'status of the law (relating to wiretapping and electronic surveillance)'" had become "'intolerable.'" S. Rep. No. 90-1097, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 (1968) ("Report") (citation omitted). In the meantime, "[t]he tremendous scientific and technological developments that [had] taken place in the last century [had] made possible [in 1968] the widespread use and abuse of electronic surveillance techniques." *Id.* at 2154. "As a result of these developments," the Committee stated, "privacy of communication is seriously jeopardized by these techniques of surveillance. Commercial and employer-labor espionage is becoming widespread. It is becoming increasingly difficult to conduct business meetings in private. Trade secrets are betrayed. Labor and management plans are revealed." *Id.*

Accordingly, Congress enacted the Wiretap Act with "dual purpose[s]": "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." *Id.* at 2153. "To assure the privacy of oral and wire communications," the Wiretap Act, as originally enacted, prohibited, with a handful of narrowly tailored exceptions, "all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers engaged in the investigation or prevention of specified types of serious crimes, and only after authorization of a court order obtained after a showing and finding of probable cause." *Id.*

In short, in order to authorize the interception of wire or oral communications under the Wiretap Act (both as originally enacted and at present), government agents must obtain a court order that "is in essence a special kind of search warrant." 1 WIRETAPPING § 1:10, at 1-17. The Act "requires an application for an interception order to establish probable cause" to believe that particular communications regarding a specified offense will be intercepted; but, the Act also "interpose[s] several extra-constitutional requirements." *Id.* § 1:10, at 1-18.

As originally enacted, the Wiretap Act governed only interception of wire and oral communications, both of which essentially are limited, by definition, to communication that is received auditorily.[17] However, in 1986 Congress passed the Electronic Communications

[17] The statute includes the following definitions, 18 U.S.C. § 2510(1)-(2):

> (1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the

Privacy Act ("ECPA"), Pub. L. 99-508, 100 Stat. 1848 (1986), which substantially revised the Wiretap Act and also enacted a new set of statutory provisions, known as the Stored Communications Act, codified at 18 U.S.C. §§ 2701 *et seq.*

ECPA added a new category of communications protected from unauthorized interception under the Wiretap Act: the category of "electronic communication," which "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," 18 U.S.C. § 2510(12), but excludes, by definition, "any wire or oral communication." *Id.* § 2510(12)(A). Thus, the current version of the Wiretap Act bars (among other things) any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procure[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," except "as otherwise specifically authorized" under the Wiretap Act. *Id.* § 2511(1)(a).

As noted, ECPA also enacted the Stored Communications Act, a set of new provisions "regulating disclosure and access to stored wire and electronic communications." 1 WIRETAPPING § 7:1, at 7-4. "The statute makes it a crime to access stored wire or electronic communications without legal authorization." *Id.* § 7:1, at 7-5. Although, "more than two decades . . . after the statute was enacted, there is still uncertainty as to precisely what it covers and protects," the "prevailing view is that it protects e-mails and similar electronic

---

> transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
>
> (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication[.]

communications stored with a public [internet service provider] after they have been received and opened by the recipient." *Id.* § 7:1 at 7-4 to -5.

The standard for legal authorization under the Stored Communications Act is in some respects less exacting than the standard to obtain an interception order under the Wiretap Act, however. To obtain access to "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less," a government entity must obtain a warrant. 18 U.S.C. § 2703(a). However, to obtain judicial authorization to access communications stored for more than 180 days, a government entity need only "offer[ ] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

The parties agree that the chat messages transmitted via the Free6.com chat service qualify as "electronic communications" under the Wiretap Act and the Stored Communications Act. Defendant argues that, by accessing the chat messages at issue, SA Burdick either intercepted electronic communications within the meaning of the Wiretap Act or, in the alternative, accessed stored communications within the meaning of the Stored Communications Act. Because SA Burdick did not obtain a warrant or an order under 18 U.S.C. § 2703(d) authorizing the interception or access,[18] defendant contends that the government violated one or both statutes.

[18] Given that the messages obviously had been in storage for fewer than 180 days, it appears that the Stored Communications Act would require a warrant to access the messages

The government responds that, because SA Burdick did not access the chat messages in real time, he did not "intercept" an electronic communication within the meaning of the Wiretap Act. As to the merits of the Stored Communications Act claim, the government contends that SA Burdick's perusal of the chat messages came within two statutory exceptions to the requirement to obtain a warrant or court order to access stored communications. First, the government argues that SA Burdick's access was "authorized . . . by the person or entity providing [the] wire or electronic communications service" at issue, *i.e.*, Free6.com (through its administrator Stefan), so as to come within the exception codified at 18 U.S.C. § 2701(c)(1). Second, the government maintains that SA Burdick's access was "authorized . . . by a user of [the wire or electronic communications] service with respect to a communication of or intended for that user," under 18 U.S.C. § 2701(c)(2). In particular, the government claims that defendant's acceptance of the terms of the warning banners on the Free6.com chat service constituted his consent to permit government agents to access his chat messages.

I need not resolve the merits of the parties' arguments and determine whether SA Burdick violated either the Wiretap Act or the Stored Communications Act. This is because, as the government points out, a violation of either statute is irrelevant to this proceeding. Regardless of which statute applies, even if the statute was violated, exclusion of evidence is not an available remedy for a violation of either statute under the circumstances here.

Neither the Wiretap Act nor the Stored Communications Act includes a statutory suppression remedy for violations in connection with "electronic communications." *See* 18

---

under 18 U.S.C. § 2703(a), rather than a mere § 2703(d) order, unless an exception to the statutory warrant requirement applied.

U.S.C. § 2515; 18 U.S.C. § 2708. The Wiretap Act contains a suppression remedy, but it is expressly limited to "wire or oral communication." The statute states, 18 U.S.C. § 2515:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

When the ECPA was enacted, adding protections for electronic communications to the statute, Congress did not see fit to adopt a statutory suppression remedy for unauthorized interception of electronic communications. Similarly, the Stored Communications Act contains no suppression remedy. Indeed, it states: "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 28 U.S.C. § 2708.

Despite the absence of an explicit suppression remedy in either statute, defendant argues that the Court should imply one in this instance. The leading decisions upon which defendant relies are the two Supreme Court decisions in the *Nardone* case. *See Nardone v. United States*, 302 U.S. 379 (1937) ("*Nardone I*"); *Nardone v. United States*, 308 U.S. 338 (1939) ("*Nardone II*").

In *Nardone*, federal agents tapped the defendants' telephones, in violation of a predecessor statute to the Wiretap Act, which provided that "'no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.'" *Nardone I*, 302 U.S. at 381 (quoting statute). At trial, "federal agents testified to the substance of

[defendants'] interstate communications overheard by the witnesses who had intercepted the messages by tapping telephone wires." *Id.* at 380. The Supreme Court rejected the government's argument that the statute should be read not to apply to agents of the federal government, *see id.* at 381-84, and remanded for a new trial. The Court reasoned that the witnesses could not testify at trial to the content of the intercepted communications because "[t]o recite the contents of the message in testimony before a court is to divulge the message," and "the act forbids such testimony." *Id.* at 382.

At the second trial, the district court precluded the defendants from "'examin[ing] the prosecution as to the uses to which it had put the information'" that it had gleaned from the unlawful wiretaps. *Nardone II*, 308 F.3d at 339 (citation omitted). The defendants were again convicted, and the question they presented on appeal was "whether or no[t] [the statute] merely interdicts the introduction into evidence in a federal trial of intercepted telephone conversations, leaving the prosecution free to make every other use of the proscribed evidence." *Id.* The Supreme Court again remanded for a new trial, reasoning that to "forbid the direct use of methods" that violated the statute "but to put no curb on their full indirect use would only invite the very methods deemed" unlawful. *Id.* at 340. This was the genesis of the "fruit of the poisonous tree" doctrine. *Id.* at 341.

In my view, the *Nardone* decisions cannot do the work defendant assigns them. Although defendant characterizes the statute at issue in *Nardone* as not containing a "suppression remedy," the *Nardone* Court based its decision to suppress the evidence on the plain text of the statute, which prohibited not only intercepting communications but divulging the content of intercepted communication as well. Moreover, even if the *Nardone* decisions do stand as

examples of the Court fashioning a judge-made exclusionary rule to address the violation of a statute that does not contain an explicit suppression remedy, subsequent Supreme Court case law has rejected that approach.

The modern rule, espoused by the Supreme Court and the Fourth Circuit, is that "[t]he availability of the suppression remedy for . . . statutory, as opposed to constitutional, violations . . . turns on the provisions of [the statute] rather than the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights." *United States v. Donovan*, 429 U.S. 413, 432 n.22 (1977) (applying statutory suppression remedy of the Wiretap Act); *see United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011) (rejecting exclusionary rule under Stored Communications Act and stating: "In the statutory context, suppression is a creature of the statute, and its availability depends on the statutory text[.]"); *accord United States v. Abdi*, 463 F.3d 547, 556 (6th Cir. 2006) ("[T]here is no exclusionary rule generally applicable to statutory violations.").[19]

Even if there might be reason to infer a suppression remedy for a statutory violation in the context of other statutes, the case for such a judge-made remedy is particularly weak in the context of the Wiretap Act and the Stored Communications Act. As the Fourth Circuit observed in *Clenney*, 631 F.3d at 667: "Congress has shown that it knows how to create a statutory suppression remedy. It did so in 18 U.S.C. § 2515." But, that remedy was only as to unlawful

[19] In addition to the *Nardone* decisions, defendant cites a handful of other decisions in which a judge-made suppression remedy has been applied to address a violation of a statute or rule in other contexts. *See Miller v. United States*, 357 U.S. 301, 313-14 (1958); *Mallory v. United States*, 354 U.S. 449, 455-56 (1957); *McNabb v. United States*, 318 U.S. 332 (1943); *Upshaw v. United States*, 335 U.S. 410, 412 (1948); *United States v. Chemaly*, 741 F.2d 1346, 1353-54 (11th Cir. 1984); *United States v. Soto-Soto*, 598 F.2d 545 (9th Cir. 1979). But, these cases cannot overcome the Supreme Court and Fourth Circuit decisions in *Donovan* and *Clenney*, which addressed the statutes at issue here.

interception of wire and oral communications. When the ECPA was enacted, Congress chose not to extend the statutory suppression remedy for wiretap violations to cover unlawful interception of electronic communications, nor did it impose an exclusionary rule for violations of the Stored Communications Act. Indeed, Congress made clear its intention that there *not* be a suppression remedy in the Stored Communications Act. As noted, it said: "The remedies and sanctions described in this chapter are *the only judicial remedies and sanctions* for nonconstitutional violations of this chapter." 28 U.S.C. § 2708 (emphasis added).

To be sure, at least one scholar in the field has argued that it was unwise for Congress to omit a suppression remedy for unlawful interception or access of electronic communications. *See* Orin Kerr, *Lifting the "Fog" of Internet Surveillance Law: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003). But, the choice was Congress's to make. This Court does not have the authority to create a suppression remedy where Congress has deliberately omitted one.

In sum, even if I were to find that SA Burdick violated the Wiretap Act or the Stored Communications Act, it would make no difference here. This is because there is no suppression remedy for a violation of either statute in connection with electronic communications. Defendant's only potential avenue for suppression is the exclusionary rule in the context of a violation of the Fourth Amendment.

According to the government, Bode's Fourth Amendment claim is flawed in several respects. First, the government argues that defendant did not have a reasonable expectation of privacy in his chat messages. Therefore, in its view, when SA Burdick perused the messages, no "search" occurred within the meaning of the Fourth Amendment. Second, the government

contends that, by indicating his acceptance of the terms stated on the two banners when logging into the Free6.com chat service, Bode consented to the disclosure of his logged chat messages to the government. Third, the government argues that, regardless of the efficacy of Bode's purported consent, Free6.com had sufficient "common authority" over its own logs to allow it to disclose them to the government. *See* ECF 67 at 2.

At the outset of the hearing on May 7, 2013, the government conceded that, by providing SA Burdick with administrative access to the website and altering the text of the banners at Burdick's request, Free6.com effectively became an agent of the government. Nevertheless, the government maintains that Free6.com's status as its agent does not affect the viability of any of its arguments concerning defendant's Fourth Amendment claim.

Notably, the government also conceded, for purposes of the Motion, that the users of at least some kinds of online messaging services (the example the government used was the "Gmail" email service offered by Google) are, as a general matter, entitled to a reasonable expectation of privacy in their use of those services and thus eligible for protection under the Fourth Amendment. This concession is in accord with precedent from the Fourth Circuit and elsewhere. For instance, in *United States v. Hamilton*, 701 F.3d 404 (4th Cir. 2012), albeit in the context of a claim of marital privilege rather than a Fourth Amendment claim, the Fourth Circuit endorsed the notion of a reasonable expectation of privacy in email, stating: "[E]mail has become the modern stenographer. . . . [E]mails today, 'in common experience,' are confidential." *Id.* at 408 (citation omitted). The *Hamilton* Court also quoted, with approval, an American Bar Association report "noting that email 'pose[s] no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable

expectation of privacy' and so there is generally 'a reasonable expectation of privacy in its use.'" *Id.* (citation omitted).

Other courts are in accord. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding "that a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [internet service provider]'") (citation omitted);[20] *see also In re Applications for Search Warrants for Information Associated with Target Email Address*, Nos. 12-MJ-8119-DJW & 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider."); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) ("'We recognize individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.'") (quoting *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011), in turn citing *Warshak*); *State v. Hinton*, 280 P.3d 476, 483 (Wash. App. 2012) (holding "that text messages deserve privacy protection similar to that provided for letters" under the Fourth Amendment); *R.S. ex rel. S.S. v. Minnewaska Area School Dist., No. 2149*, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (holding "that one cannot distinguish a password-protected private Facebook message from other forms of private electronic

[20] As a corollary to its holding, the *Warshak* Court also said that, "to the extent that the [Stored Communications Act] purports to permit the government to obtain such emails warrantlessly," *i.e.*, pursuant to an order under 18 U.S.C. § 2703(d), when the emails have been in storage for more than 180 days, "the [Stored Communications Act] is unconstitutional." *Warshak*, 631 F.3d at 288.

correspondence," and thus, "based on established Fourth Amendment precedent, that R.S. had a reasonable expectation of privacy to her private Facebook information and messages").

Nevertheless, the foregoing case law does not dictate that Mr. Bode had a reasonable expectation of privacy in the chat messages at issue here. To begin with, the cases finding a reasonable expectation of privacy in email or similar electronic communication have been premised on the private, person-to-person nature of the communication, akin to a letter. In contrast, "one's 'reasonable expectation of privacy' cannot encompass anything exposed to the public . . . ." *Ostergren v. Cuccinelli*, 615 F.3d 263, 282 (4th Cir. 2010) (citing *California v. Greenwood*, 486 U.S. 35 (1988)).

Although some of the chat messages that SA Burdick read were private messages sent from defendant to other individual users, many of the messages were posted in public chat rooms, where any user of the Free6.com chat service who was logged in could have viewed them (notably, including every posting of the "-11 radator.jpg" image). "Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Messages sent to the public at large in [a] 'chat room' . . . lose any semblance of privacy." *United States v. Maxwell*, 45 M.J. 406, 418-19 (C.A.A.F. 1996). As one district court observed, in rejecting a claim of Fourth Amendment protection for messages posted in publicly accessible online chat rooms hosted by the internet service provider America Online ("AOL"), the defendant "could not have a reasonable expectation of privacy in the chat rooms," because "when Defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent." *United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).

Courts have reached the same conclusion with respect to other electronic communications that, by their nature, are readily viewable by the public. *See, e.g.*, *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir.) (holding that defendant had no reasonable expectation of privacy in files on his computer shared over a peer-to-peer file sharing network, because defendant "was clearly aware that LimeWire was a file-sharing program that would allow the public at large to access files in his shared folder unless he took steps to avoid it," and his "files were . . . entirely exposed to public view; anyone with access to LimeWire could download and view his files without hindrance") (citing *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008), *cert. denied*, ___ U.S. ___, 129 S. Ct. 2037 (2009)), *cert. denied*, ___ U.S. ___, 131 S. Ct. 795 (2010); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (same), *cert. denied*, 559 U.S. 915 (2010). Accordingly, I conclude that defendant had no reasonable expectation of privacy in messages he sent to public chat rooms on the Free6.com chat service.

Defendant's private messages to other individual users of the chat service, which are more akin to email, present a somewhat closer question. However, much if not all of the case law, cited *supra*, which has recognized the possibility of a reasonable expectation of privacy in email, has also recognized that whether a user has a reasonable expectation of privacy in an electronic communications stored or transmitted by a third-party service can be affected by the terms of service at issue. Although the Fourth Circuit reasoned in *Hamilton* that "one may generally have a reasonable expectation of privacy in email," 701 F.3d at 408, the defendant in that case did not. The defendant's email account was provided by his employer, which had adopted a computer usage policy that "expressly provide[d] that users have 'no expectation of privacy in their use of the Computer System' and '[a]ll information created, sent[,] received,

accessed, or stored in the . . . Computer System is subject to inspection and monitoring at any time.'" *Id.* (quoting policy). Moreover, the defendant "had to acknowledge the policy by pressing a key to proceed to the next step of the log-on process, every time he logged onto his work computer." *Id.* Therefore, the Court reasoned that the case was analogous to an earlier case in which the Fourth Circuit "held that a defendant did not have an 'objectively reasonable' belief in the privacy of files on an office computer after his employer's policy put him 'on notice' that 'it would be overseeing his Internet use.'" *Id.* at 408-09 (quoting *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000)).

The *Simons* case, cited in *Hamilton*, is also relevant. In that case, the defendant, a government employee, was prosecuted for child pornography offenses after images of child pornography were discovered on his government-issued computer. *See Simons*, 206 F.3d at 395. The agency that employed the defendant had instituted an internet usage policy for its employees that, among other things, "specifically prohibited" accessing "unlawful material," required employees to use the internet "for official government business only," and warned employees that the agency conducted extensive "electronic audits" of usage in order "'to support identification, termination, and prosecution of unauthorized activity.'" *Id.* (quoting policy). The pornographic images at issue were discovered on the defendant's computer as a result of such auditing. *See id.* at 396. After the defendant was convicted, he appealed, challenging the admission of the images on Fourth Amendment grounds.

The Fourth Circuit stated: "Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets. However, office practices, procedures, or regulations may reduce legitimate privacy expectations." *Id.* at

398 (internal citations omitted). "[I]n light of the Internet policy," the Fourth Circuit ruled that the defendant "lacked a legitimate expectation of privacy in the files downloaded from the Internet" onto his employer-issued computer. *Id.* The Court reasoned that the policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private." *Id.*

Similarly, in *Warshak* the Sixth Circuit "acknowledge[d] that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account." 631 F.3d at 286. In reasoning that is instructive here, the court "observed that the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.* (emphasis in original). Moreover, the court held that the subscriber agreement in that case, which stated that the defendant's internet service provider "'may access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service,'" *id.* at 287 (quoting subscriber agreement), did not "diminish the reasonableness of Warshak's trust in the privacy of his emails." *Id.* But, the Sixth Circuit was "unwilling to hold that a subscriber agreement will never be broad enough to snuff out a reasonable expectation of privacy," and opined that, if the internet service provider "expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable." *Id.* (citation omitted).

Here, the warning banners that users of the Free6.com chat service saw each time they logged in stated: "Child pornography or other illegal material will immediately be reported to the posters [sic] local authorities"; "All posted pictures and conversations, public and private, are

logged and supervised"; and "Free6 may disclose these communications to the authorities at its discretion."[21] This is similar to the computer policy in *Hamilton*, which was found to defeat the employee's reasonable expectation of privacy. As noted, in *Hamilton* the policy stated: "'All information created, sent[,] received, accessed, or stored in the . . . Computer System is subject to inspection and monitoring at any time.'" 701 F.3d at 408 (quoting policy). It is also similar to, if not more stringent than, the banner hypothesized in *Warshak*, stating that the service provider would "'audit, inspect, and monitor' its subscriber's emails," which the *Warshak* Court said "might" negate a reasonable expectation of privacy. *Warshak*, 631 F.3d at 287. And, it is clearly more stringent than the policy that the service provider "'may access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service,'" *id.* at 287 (quoting subscriber agreement), which the *Warshak* Court held did not negate a reasonable expectation of privacy.

To argue that the banners here did not negate a reasonable expectation of privacy, defendant principally relies on an unreported district court decision in *United States v. Sims*, No. CR-00-193-MV, 2001 WL 36498440 (D.N.M. Apr. 19, 2001), *aff'd in part, rev'd in part*, 428 F.3d 945 (10th Cir. 2005). In that case, the district court held that a warning banner on a government employee's computer system did not "waive [the employee's] expectation of privacy as against law enforcement." *Id.* at *8. The warning banner stated, *id.* at *9:

> This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system

[21] The quoted language includes the language added to the second banner after Stefan revised it at SA Burdick's request. Because the revised language is what was in effect in January 2010 when Mr. Bode allegedly logged in to the chat service and sent the chat messages at issue, the revised language is the only language that is relevant to Bode's expectation of privacy.

> and files on this system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness and consent to these terms and conditions. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

The district court reasoned that "an employee may not have an expectation of privacy against his employer but may retain that expectation against law enforcement." *Id.* It continued, *id.* at *10:

> By the terms of the banner itself, it is not an effective "waiver" of Mr. Sims' Fourth Amendment right to be free from unreasonable searches and seizures as against law enforcement. The language of the banner only allows "authorized site or Department of Energy" personnel to monitor the computer. The banner makes no mention that law enforcement may monitor the computer. The fact that the warning states that the employer may disclose the results of a search to law enforcement merely reiterates the unremarkable principle that "Fourth Amendment concerns simply are not implicated 'when a private person voluntarily turns over property belonging to another and the government's direct or indirect participation is nonexistent or minor.'" (Citation omitted.)

Moreover, as the district court saw it, "[e]ven if the banner were to be interpreted as waiving employees' expectation of privacy against law enforcement, the Court would find that the waiver was unenforceable, for it would eviscerate Fourth Amendment protections beyond what has been recognized as reasonable." *Id.* It concluded: "The Government may not eliminate citizens' expectation of privacy simply by making an announcement that they have none." *Id.*

Nevertheless, the district court determined that, "[e]ven without the knowledge from the . . . illegal search of Mr. Sims' office computer, the FBI still had sufficient information to present to the Magistrate that there were images of child pornography on Mr. Sims' office

computer." *Id.* at *16. Accordingly, the evidence derived from a subsequent search pursuant to a warrant was not suppressed, and the defendant was subsequently convicted.

On appeal, the Tenth Circuit affirmed Sims' conviction.[22] *See United States v. Sims*, 428 F.3d 945 (10th Cir. 2005). In a footnote, the appellate court observed, *id.* at 954 n.3:

> In this appeal, the Government argues that the district court's decision that this warrantless search was illegal was wrong in light of this court's subsequent decision in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002). In *Angevine*, we held that a university professor did not have any reasonable expectation of privacy in his office computer; however, we emphasized that this issue requires a case-by-case analysis. *Id.* at 1134-35.

Nevertheless, the Tenth Circuit determined that it "need not decide" whether the warrantless search was unlawful. *Id.* This was because it affirmed the district court's determination that the subsequent warrant was supported by probable cause, even after the information gleaned from the warrantless search was excised. *See id.* at 954.

The computer use policy in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), like the one in *Sims* (and in this case), warned that system administrators could monitor usage and would turn over evidence of illegality to law enforcement. But, it did not explicitly warn users that law enforcement might be given direct access to the computer system. *Id.* at 1132-33 (quoting and describing computer use policy). The *Angevine* Court stated: "[W]e have never held the Fourth Amendment protects employees who slip obscene computer data past network administrators in violation of a public employer's reasonable office policy." *Id.* at 1135. It concluded that "Angevine could not have an objectively reasonable expectation of privacy," *id.*,

[22] For reasons that are not germane here, the court vacated the sentence and remanded for resentencing.

and therefore affirmed the district court's conclusion that "police did not need a search warrant to seize [Angevine's] University computer." *Id.* at 1132.

Regardless of how the Tenth Circuit might have ruled in *Sims* if it had to decide the issue, the district court decision in *Sims* is incompatible with Fourth Circuit precedent, such as *Hamilton* and *Simmons*, discussed *supra*, which concluded that warning banners analogous to those posted on Free6.com deprived users of a reasonable expectation of privacy in their use of the computer systems at issue. Moreover, the Tenth Circuit in both *Sims* and *Angevine* emphasized the case-by-case nature of the inquiry into an employee's "expectation of privacy in the workplace." *Angevine*, 281 F.3d at 1134; *see Sims*, 428 F.3d at 954 n.3.

Therefore, I conclude that Free6.com's warning banners deprived Mr. Bode of any reasonable expectation of privacy in his chat messages. As a result, SA Burdick's review of Bode's logged messages did not constitute a search within the meaning of the Fourth Amendment.

In the alternative, even if SA Burdick's review of the messages constituted a search, Bode's acceptance of the terms stated in the second warning banner was sufficient to constitute his consent to the search. As noted, the second banner stated, in pertinent part: "All posted pictures and conversations, public and private, are logged and supervised. Free6 may disclose these communications to the authorities at its discretion." Like every user of the chat service, on each occasion that Bode logged in, he was required to click a button labeled "ACCEPT" immediately below the stated terms.

"[C]onsent to search provides an exception to the Fourth Amendment's warrant and probable cause requirements. Once a defendant voluntarily gives consent, a search that falls

within the scope of that consent is constitutionally permissible." *United States v. Ortiz*, 669 F.3d 439, 445 (4th Cir. 2012).

Defendant argues that SA Burdick's review of the logged messages was outside the scope of any purported consent. As defendant sees it, "the scope of Mr. Bode's consent to search his communications related only to free6—**not** the government." Reply at 3 (emphasis in original). He relies on *Reedy v. Evanson*, 615 F.3d 197, 229-30 (3d Cir. 2010), in which the court held that government agents exceeded the scope of the plaintiff's consent when they performed drug testing on a blood sample that the plaintiff, who had just been sexually assaulted, had consented to have drawn as part of a "rape kit examination," to test for sexually transmitted diseases and evidence concerning her attacker.

I am not persuaded by defendant's view of the language of the second banner. The banner clearly stated that Free6.com logged all of the chat messages sent and received via the service, both public and private, and stated that, in its discretion, Free6.com could turn those messages over to "the authorities." At least for purposes of this case, there is no meaningful distinction between giving a copy of the log to SA Burdick, on the one hand, and giving SA Burdick access to view the copy of the log stored on Free6.com's servers, on the other hand.[23] Thus, Mr. Bode's consent to search is an independent basis on which to reject his Fourth Amendment claim.

In light of my acceptance of the government's first two arguments—that there was no reasonable expectation of privacy and, in the alternative, that defendant consented to the

[23] Conceivably, a meaningful distinction might be present if real-time interception of communications were involved. But, as I have already concluded, real-time interception did not occur in this case.

search—I need not resolve the government's additional argument that Free6.com had common authority to consent to the search of the logs.

For all of the foregoing reasons, defendant's Motion to Suppress Evidence (ECF 32) is denied by the Order that accompanies this Memorandum Opinion.[24]

Date: August 21, 2013

/s/
Ellen Lipton Hollander
United States District Judge

[24] In light of my ruling with respect to the Motion to Suppress Evidence, the issues in connection with the Motion to Suppress Statements and the *Franks* Motion, on which I reserved ruling in my Order of May 9, 2013 (ECF 65), are rendered moot.