UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
VS.	§	CRIMINAL ACTION
	§	NO. 3:13-CR-20
DONALD JOHN POST SR	§	

MEMORANDUM AND ORDER

Child pornography was uploaded to a website. Federal agents obtained the image from the website and used its metadata to identify the GPS coordinates where the photo had been taken with an iPhone. That metadata led the agents to the home of Defendant Donald Post, who then admitted to taking that photo, as well as others, of a four-year-old girl who had recently stayed at his home. Post now contends that even though he had uploaded the image to a website, he retained a privacy interest in that image's metadata that law enforcement invaded in violation of his Fourth Amendment rights.

I. BACKGROUND

A. Agents Discover The Image

During the course of their investigation into child exploitation activities, FBI agents discovered a website dedicated to the advertisement and distribution of child pornography. On that website, a user posted a picture containing child pornography. The image shows what appears to be an adult male's hand pulling

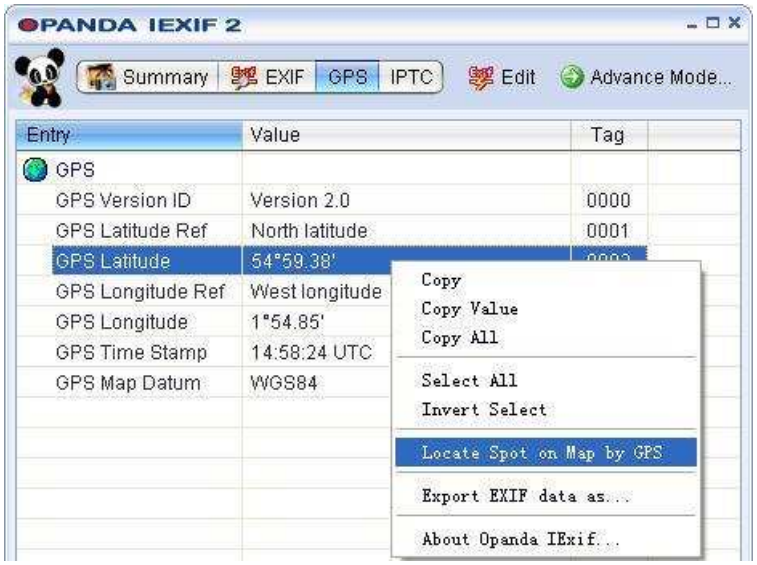
aside the underwear of a prepubescent girl, with the focus on the exposed genitals. The image also revealed a portion of a white leather couch on which the child appeared to be sleeping. Other than the clue that the house where the photo was taken contained a white leather couch, the image provided no indication of where in the world the photo was taken. And the often fruitful internet protocol (IP) address was not helpful because the user had connected to the internet through a special browser designed to make the user's IP address anonymous.

B. Metadata Provides GPS Coordinates

Another source of information—data that was embedded in the photo, called metadata—provided the answer to the needle-in-the-haystack problem the agents faced. Metadata, most commonly associated with electronic documents where it can identify when a document was created and by which user, is "data that is stored internally in a file . . . not explicitly defined by the user." Sharon D. Nelson and John W. Simek, *Too Much Information: Photos taken with a digital camera contain metadata. Should you care?*, Texas Bar Journal, Jan. 2014, at 14. In digital photos, metadata typically includes "the date and time the photo was taken; camera settings, such as aperture and shutter speed; manufacturer make and model . . . and—in the case of smartphones—the GPS coordinates of where the photo was taken." *Id.* In most cases, this information is automatically embedded in digital pictures unless the user opts out of the features that capture the

information. For instance, the Apple iPhone automatically captures the coordinates of where a picture is taken unless the user turns off the iPhone's geotagging feature.

Several free websites allow users to see this metadata, also called Exif (Exchangeable image file format). For instance, users of the website opanda.com can download the site's free software and use it to view an image's metadata.



Screenshot from opanda.com revealing the GPS coordinates embedded in a digital photograph.

Agents used opanda.com to search the photo they had discovered on the website. Within minutes of accessing the site, opanda.com revealed that the image was taken at GPS coordinates 29 deg 29.4400 N 95 deg 9.7400 W, on an Apple iPhone 4, at 00:55:11 on July 23, 2013. Tracking those GPS coordinates with Yahoo Maps, agents determined that the picture was taken at a home in League City, Texas.

C. Agents Find Post

At the first house the agents visited, the residents indicated that they did not have an Apple iPhone 4 or a leather couch similar to the one in the image, nor had any children recently been in their home. After the agents explained the purpose of their visit, the residents revealed that a registered sex offender lived in a house nearby. The agents then verified the residents' statement by checking a sex offender database. They learned that Donald Post, a registered sex offender, lived in a home about 100 feet from the first address, within the range of error of the GPS location generated by the iPhone's automatic geotagging feature.

The agents knocked on Post's door and he granted them permission to enter his home.[1] Inside, the agents observed that the couch in Post's home matched the one in the photo. Post agreed to talk to the agents and admitted that he took the image with his iPhone 4 and uploaded it to the internet. He told the agents that he took approximately ten photos of the four-year-old girl during her recent stay at his home. The officers then searched Post's belongings, with his consent, and found other images of suspected child pornography. This case followed.

II. DID THE SEARCH FOR METADATA VIOLATE THE FOURTH AMENDMENT?

In his suppression motion, Post acknowledges that he had no expectation of

[1] At the suppression hearing, Post also argued that he did not voluntarily consent to allow the officers to enter his home. The Court orally denied this claim during the hearing and need not expand on that ruling in this order.

privacy in the image that he uploaded to the website, but contends that he did retain a privacy interest in the embedded metadata because he did not realize he was releasing that information and he intended to remain anonymous. In other words, he would split the image into two distinct parts, one of which the government could obtain because it was placed in the public domain and one of which it could not.

Whether a search implicates the Fourth Amendment "depends on (1) whether the defendant is able to establish an actual, subjective expectation of privacy with respect to the place being searched or items being seized, and (2) whether that expectation of privacy is one which society would recognize as reasonable." *United States v. Gomez*, 276 F.3d 694, 697 (5th Cir. 2001). As he concedes, Post had no expectation of privacy in the image itself, which he published on a website for third parties to view. *See United States v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011) (holding that defendant had no expectation of privacy in image he placed in peer-to-peer file sharing program); *United States v. Dodson*, --- F. Supp. 2d ----, 2013 WL 4400449, at *3 (W.D. Tex. Aug. 13, 2013) ("Defendant did not have an actual, subjective expectation of privacy because Defendant had already exposed the entirety of his files to the many unknown users on the [file-sharing network], which is the exact opposite of exhibiting an expectation of privacy.").

Post's attempt to carve out the metadata from his public release of the image finds no support in the text of the Fourth Amendment or the case law applying it. The Fourth Amendment protects privacy interests in places and things. The Reasonableness Clause refers to the "right of the people to be secure in their persons, houses, *papers*, and *effects*." U.S. Const. amend. IV (emphasis added). The Warrants Clause requires a particular description of "the place to be searched, and the persons or *things* to be seized." *Id.*; *see also Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) ("The Fourth Amendment 'indicates with some precision the places and things encompassed by its protections': persons, houses, papers, and effects." (citing *Oliver v. United States*, 466 U.S. 170, 176 (1984))). The "effect" or "thing" in this case is the electronic image Post took on his iPhone. He gave up his right to privacy in that image once he uploaded it to the internet, and that thing he publicly disclosed contained the GPS coordinates that led agents to his home. There is no basis for divvying up the image Post uploaded into portions that are now public and portions in which he retains a privacy interest.

The application of the Fourth Amendment to modern technology can present novel issues. *See, e.g., Kyllo v. United States*, 533 U.S. 27 (2001) (determining whether use of a thermal imaging device to monitor heat radiating from person's home was a search). But other times traditional Fourth Amendment principles provide a straightforward answer once the veneer of technological complexity is

removed.[2] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1007 (2010) ("Technology neutrality assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world. That is, courts should try to apply the Fourth Amendment in a new environment in ways that roughly replicate the role of the Fourth Amendment in the traditional physical setting."). The latter characterizes Post's arguments that a Fourth Amendment violation occurred because he lacked knowledge that the photo he disclosed contained metadata and because he retained an interest in the anonymity of the image.

A hypothetical based on a technology that was novel and revolutionary not that long ago but that is now widespread—DNA—dispels both of these arguments. Assume a defendant left an article of his clothing at a crime scene in 1981. At the time, the defendant had no idea that years later crime labs would be able to conduct DNA analysis of hairs present on that clothing. And in leaving the clothing, he certainly intended to do so "anonymously." On those grounds, would the defendant be able to suppress the results of the DNA analysis? Of course not, because he left the clothing in a public place and lost any expectation of privacy he

[2] The same is true for the rules of evidence, where traditional principles are commonly applied to the admissibility of electronic information. *See, e.g.*, *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) (one of the first cases to thoroughly address the traditional rules of evidence as applied to electronically stored information).

had in it, regardless of how he contemplated that clothing could be used. The same would have been true if in an earlier age a defendant had tried to argue that he meant to leave a cigarette butt in a public space, but had not intended to leave his latent fingerprint that law enforcement used to identify him. And the same is true for the image that Post uploaded to the website: once it was left in a public place, he no longer had a Fourth Amendment privacy interest in it. *Cf. United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (holding that ineffectual attempt to prevent peer-sharing website from sharing his files did not give defendant an expectation of privacy because his files "were still entirely exposed to public view").

It is worth mentioning that this case does not implicate two Fourth Amendment issues that are currently receiving significant attention. Two district courts recently handed down conflicting opinions concerning the constitutionality of the National Security Agency's bulk collection of telephone metadata. *Compare Klayman v. Obama*, --- F. Supp. 2d ----, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (finding Fourth Amendment violation), *with Am. Civil Liberties Union v. Clapper*, --- F. Supp. 2d ----, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (finding same metadata collection program constitutional). Whatever the ultimate outcome of that issue in higher courts, whether an individual lacks a privacy interest in dialed numbers because those numbers are necessarily disclosed to his phone

company is a much different question than whether an individual loses his privacy interest in an item because he voluntarily makes it publicly available on the internet.[3] Second, earlier this month the Supreme Court decided to resolve a split in the lower courts concerning whether the search incident to arrest doctrine that allows law enforcement to seize the cellphone of an arrestee also allows a warrantless search of the seized phone. *See United States v. Wurie*, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, 2013 WL 4402108 (U.S. Jan. 17, 2014); *People v. Riley*, 2013 WL 475242 (Cal. Ct. App. 2013), *cert. granted*, 2013 WL 3938997 (U.S. Jan. 17, 2014). At first glance it might seem that the courts recognizing a distinction between seizing the phone and searching its contents lend support to Post's attempts to divvy up his privacy interests in the photo. But the cases the Supreme Court is reviewing are not about whether an arrestee has a privacy interest in a cellphone found in his possession. He maintains such an interest in both the phone and its contents. The issue is whether the justifications that overcome that privacy interest and allow for warrantless seizure of the phone also support warrantless search of its contents. Post, by contrast, had no cognizable privacy interest that the government needed to overcome to justify searching for metadata in the photo he placed on the internet.

[3] Unlike freely accessible sites like Google or Yahoo, users of the website where Post displayed the picture have to download a special browser, called a TOR browser, to gain access to the site. But that browser is available for any internet user to utilize and is the only barrier that would prevent someone from accessing the website.

III. CONCLUSION

Post shared an illicit image on what is today perhaps the most public medium imaginable—the internet—so that others could see it. For the reasons explained above, he did not have a privacy interest in the metadata embedded in that image, and the government did not engage in an unconstitutional search when it used that metadata to find him. Accordingly, Post's Motion to Suppress (Docket Entry No. 20) is **DENIED**.

SIGNED this 30th day of January, 2014.

Gregg Costa
United States District Judge