The Private Search Doctrine is Still Subject to the Exceptions to the Warrant Requirement

September 2018

Article Source : http://www.patc.com/weeklyarticles/2018_us_v_tolbert_chapman.pdf

In United States v. Tolbert, ___ F.Supp.3d ___, 2018 WL 3611053 (D.N.M. July 22, 2018), the United States District Court for the District of New Mexico was asked to determine a question that was specifically left unanswered by the United States Court of Appeals for the Tenth Circuit: whether the exceptions to the warrant requirement are available and are applicable to the "private search doctrine." The District Court held that the exceptions were available based upon the following facts.

Defendant Donald Alvin Tolbert was convicted in 2006 on two counts of criminal sexual contact of a child under age thirteen along with other charges. Tolbert served a term of imprisonment and, subsequently, began serving concurrent terms of probation and parole. In 2010, the state arrested Tolbert for violating the terms of his probation and parole and reincarcerated him for 330 days. Then, the state released Tolbert a second time, subject to certain conditions of probation. As part of his release, Tolbert agreed to various standard conditions of probation, including allowing any probation or parole officer to visit him at his home or place of employment at any time, and permitting a warrantless search by the officer if he or she had reasonable cause to believe that the search would produce evidence of a parole violation. As a convicted sex offender, Tolbert also promised to provide all of his email addresses, usernames, and passwords to his probation officer. Further, Tolbert agreed that any computer or electronic device to which he had access could "be examined for inappropriate content [which expressly included child pornography] at any time."

On September 1, 2012, five emails with a total of fifteen attachments were sent through American Online ("AOL") by a user with the email address of ddt123abc@aol.com which was an email address that allegedly belonging to Tolbert. Three of these emails were sent to a user with the email address of donnieisagod@aol.com which also allegedly belonging to Tolbert. The other two emails were sent to a third-party email address: widd2703@web.de. In accordance with its practice in 2012, AOL did not initially open or view the files attached to the emails.

However, by scanning the emails and attachments using software employing "hash value" matching, AOL detected the presence of suspected child pornography. A "hash value" is a unique 32-character string of alphanumeric characters that is the result of an algorithm that has been applied to a particular photograph or video. No two photographs or videos will produce the exact same 32-character hash value unless the two are identical; any change to a photo or video, no matter how small, will result in a different hash value. AOL maintains a database of hash value strings generated from photographs and videos containing known or suspected child pornography. AOL maintains a system known as "image detection filtering process," or IDFP, that scans its users' emails for hash values that are identical to those in AOL's database. AOL did not develop this system at the behest of law enforcement.

As it is required to do by law, AOL electronically submitted the five emails and corresponding CyberTip reports concerning suspected child pornography to the National Center for Missing and Exploited Children ("NCMEC"). These CyberTips provided by AOL to NCMEC included: (1) the email addresses of both the senders and the

recipients of the emails, (2) the subjects of the emails, along with all of their attachments; (3) identification of the specific attachments which had been hash value matched as child pornography; and (4) the IP address corresponding to the email sender for all five emails.

AOL's software also automatically prevented the five emails and their attachments from reaching their intended recipients and, then, terminated and saved a snapshot of the user's account. The entire process was fully automated, meaning no AOL employee opened or read the emails or attachments before AOL sent the CyberTip to NCMEC. However, in 2012, an AOL employee did open and view the email and attachments the next business day after the CyberTip was sent to NCMEC in order to confirm that the hashed image did in fact belong in AOL's database of images of child pornography.

On September 5, 2012, the NCMEC opened and viewed the five emails and their attachments forwarded by AOL (along with the CyberTips) and determined that the attachments appeared to contain child pornography. It did so without seeking or obtaining a search warrant. It then conducted various searches on various publicly available databases for the IP address associated with the five emails, for the two email addresses listed above, as well as for the names "Donnie T" and "Don Tolbert." The open source searches on the IP address were conducted in order to locate the sender in a particular geographic area—in this case, Albuquerque, New Mexico. The NCMEC then performed public, online searches on some of the information sent by AOL in the CyberTip, including the two email addresses noted above that were associated with the five emails and other unique identifiers such as "YUNGMUFFMAN," and eventually to someone named "Donnie," then "Don Tolbert," then Margaret Tolbert and her Albuquerque address, and then eventually to a Donald Alvin Tolbert in Albuquerque, New Mexico with a specific address and date of birth.

The NCMEC forwarded the CyberTip reports containing those emails and attachments, as well as the results of its public record searches, to the New Mexico Attorney General's Office, Internet Crimes Against Children ("ICAC") division. The ICAC is the clearinghouse for CyberTips with a connection to New Mexico. An analyst with the Attorney General's Office reviewed the CyberTips, including the hash-matched images, and ran open source searches regarding the associated IP address to determine that the source of the emails is in New Mexico. Then, the analyst refers the CyberTips to the Special Agent in Charge, who assigns them to law enforcement for further investigation.

On September 7, 2012, Special Agent Owen Pena of the AG's office was assigned to conduct an investigation regarding the five CyberTips relating to "Donald Alvin Tolbert." By using open source searches on the IP address associated with the email addresses of donnieisagod@aol.com and ddt123abc@aol.com listed in the CyberTip reports, Pena verified the geographical connection between the IP address and Albuquerque, New Mexico. Using that information, Pena obtained grand jury subpoenas duces tecum for information associated with the IP address from ISP CenturyLink as well as information from AOL regarding the two email addresses. After determining that the emails in the CyberTips were associated with Donald Tolbert, Pena called Tolbert's probation officer and confirmed that he was a registered sex offender on probation in New Mexico.

Thereafter, Pena contacted Christina Altamirano who is an agent with Homeland Security Investigations specializing in internet crimes against children and sexual exploitation crimes. Altamirano met with Pena and reviewed the evidence that he had obtained regarding Tolbert. This included subscriber information from AOL and Century Link as well as five NCMEC reports and associated videos. Using that evidence, Altamirano prepared and obtained search warrants for AOL regarding the two email addresses mentioned in the CyberTip reports. These warrants revealed subscriber information for the two email addresses along with IP addresses, times, and dates the accounts were used. Similarly, Pena obtained search warrants for Tolbert's residence as well as that of Tolbert's mother.

At Tolbert's residence, officials seized cell phones, a notebook, photographs, books and videos. At his mother's home, they found two computers, a digital camera, and a cell phone. Police found photos and videos depicting child pornography on the two computers seized at Tolbert's mother's home. In an interview, Margaret Tolbert told police that she and Tolbert were the only ones with access to those computers.

Finally, at the suppression hearing, Altamirano explained that, even without the emails and attachments, she still would have conducted an investigation that would have ended in obtaining the emails and attachments as well as connecting them to Tolbert.

Eventually, Tolbert was indicted, and he filed a motion to suppress the evidence obtained against him as being obtained in violation of his Fourth Amendment rights. Specifically, Tolbert argued that, under the Tenth Circuit's holding in United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016), the NCMEC is a government entity or agent and, therefore, was required to obtain a warrant prior to performing searches by opening his emails and their attachments. Tolbert claimed that, because the MCMEC did not have a warrant, the evidence obtained against him was fruit of the poisonous tree and should be suppressed.

The District Court began its consideration of Tolbert's motion to suppress by following the Tenth Circuit's holding in Ackerman and concluding that the NCMEC is a governmental entity. As a governmental entity, the NCMEC is bound by the Fourth Amendment, and therefore, any search performed by the MCMEC was subject to the Fourth Amendment's reasonableness and warrant requirements.

Next, the District Court considered whether the "private search doctrine" made the NCMEC's search permissible. The United States Supreme Court has concluded that even a "wrongful search . . . conducted by a private party does not violate the Fourth Amendment." Walter v. United States, 447 U.S. 649, 656 (1980). And, "such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." Id. In United States v. Jacobsen, 466 U.S. 109 (1984), FedEx employees opened a damaged package, found suspicious plastic bags of white powder inside, and passed the parcel to the government, along with a description of what they had found. Id. at 111. An agent from the Drug Enforcement Agency ("DEA") then repeated the same investigation, opening the package and examining its contents. Id. Finally, the DEA agent subjected the white powder to a chemical drug test to confirm that it was cocaine. Id. at 111-12.

Considering all of this, the Supreme Court held that no "search" implicating the Fourth Amendment had taken place because there was a "virtual certainty" that the government could have discovered "nothing else of significance" in the package nor learned anything beyond what it had "already . . . been told" by a private party. Id. at 119. In other words, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." Id. at 117.

Here, the District Court noted that it was bound by the Tenth Circuit's holding in Ackerman and determined that the NCMEC's search was not a private search and that the search violated Tolbert's Fourth Amendment rights because no warrant had been obtained prior to the search.

Next, the District Court considered a question left open by the Tenth Circuit in Ackerman: whether a search under these circumstances could be valid based upon any of the exceptions to the warrant requirement. The District Court concluded that the exceptions could apply and that, in this case, the good faith exception and the inevitable discovery exception applied. As such, the District Court denied Tolbert's motion to suppress.

As for the good faith exception, the District Court explained that the exception applies when law enforcement officers rely in good faith on a warrant issued by a judge or magistrate. In addition, the District Court stated

that the good faith exception applies when a law enforcement officer reasonably relies on a statutory scheme that authorizes warrantless, administrative searches, even if the statute is later found to be in violation of the Fourth Amendment.

Here, both prongs were present. Both Altamirano and Pena reasonably relied on the warrants that they obtained, having no reason to believe that the NCMEC provided the emails to AOL in violation of Tolbert's Fourth Amendment rights. Moreover, the statutory scheme during the relevant time appeared to give the NCMEC the authority to conduct searches without a warrant, and the Tenth Circuit only held that the NCMEC was a government entity some four years later. Therefore, the District Court found that the good faith exception applied and that Tolbert's motion to suppress should be denied.

Finally, the District Court held that the inevitable discovery exception to the warrant requirement applied. Under this exception, illegally obtained evidence may be admitted if it ultimately or inevitably would have been discovered by lawful means. The inevitable discovery exception applies whenever an independent investigation inevitably would have led to discovery of the evidence, whether or not the investigation was ongoing at the time of the illegal police conduct.

In this case, the District Court held that the evidence showed that law enforcement would have discovered Tolbert's receipt of child pornography regardless of any Fourth Amendment violation. Accordingly, the District Court denied Tolbert's motion to suppress.