STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS

KENT, SC. **SUPERIOR COURT**

(FILED: December 8, 2016)

STATE OF RHODE ISLAND	:	
	:	
VS.	:	**K2-2015-0533A**
	:	
ROBERT O'BRIEN	:	

DECISION

RUBINE, J. The Defendant has been charged with one count of possession of child pornography. A motion was filed by the State for an in limine determination of whether the State's introduction of the "CyberTipLine Report" (CyberTip) received by the R.I. State Police from a national reporting agency, the National Center for Missing and Exploited Children (NCMEC) is proper. The CyberTip contains information supplied to NCMEC by the internet service provider or ISP, in this case Microsoft, which identified the subject image as an example of "child pornography" by matching a file found in Defendant's Microsoft Cloud storage to an image contained in the NCMEC database. The CyberTip identifies Defendant's Microsoft Cloud account as the source of the image and links the Defendant's home IP address, e-mail address, and also the date and time associated with the upload of the image to the Defendant himself. In its introduction, the report explains that the contents of the CyberTip were submitted electronically by the "reporting person," here Microsoft Skydrive of Redmond, Washington. From the data supplied by Microsoft, NCMEC was able to confirm the image as pornographic; identify the name and address of the owner of the account in which the uploaded image was stored; the date and time of the upload; and related identifying information. This information was reported by NCMEC to the R.I. State Police by way of the CyberTip. The R.I. State Police,

believing the information was reliable and accurate, pursued its investigation leading ultimately to the Defendant being charged with possession of child pornography. The process of retrieval and reporting of the data was described generally by Detective Petit at the hearing. Detective Petit—a detective in the Warwick Police Department, as well as a member of the statewide task force on internet pornography—testified at the hearing associated with the State's motion. In summary, he testified that the police agency was provided with the CyberTip.

Detective Petit also testified as to his knowledge of the process, which this Court finds to be anecdotal. Detective Petit testified that he confirmed through telephone calls to NCMEC and Microsoft their policies and procedures, but admitted on cross-examination that he had no personal knowledge of how the data was generated. Without such personal knowledge, the defense argues that it is unable to test the reliability of the data contained in the report; nor was a witness presented who could authenticate the document. It is the unavailability of such witnesses that Defendant contends denies him the right of confrontation secured to him under the Sixth Amendment to the United States Constitution.

Analysis

The seminal case discussing the Sixth Amendment right of confrontation is Crawford v. Washington, 541 U.S. 36, 53-54 (2004). In Crawford, the United States Supreme Court held that the Confrontation Clause bars the admission of "[t]estimonial statements of witnesses absent from trial," unless the witness is unavailable or was already cross-examined. Id. at 59. Crawford states that in order to trigger the right to confrontation, the proffered evidence must first constitute hearsay. Id. at 36; United States v. Cameron, 699 F.3d 621, 641 (1st Cir. 2012); United States v. Washington, 498 F.3d 225, 229 (4th Cir. 2007). The Rhode Island Rules of Evidence define hearsay as ". . . a statement, other than one made by the declarant while

testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." R.I. R. Evid. 801(c). "A 'declarant' is a person who makes a statement." R.I. R. Evid. 801(b) (emphasis added). Based upon the Crawford test, I find the document proposed as evidence by the State to be testimonial in nature and subject to confrontation. Similarly, the information provided in the CyberTip was intended to be used for prosecutorial purpose. The information concerning the subject image and how the computer-generated information tying the image to the Defendant in the CyberTip must be tested for its reliability through cross-examination of the person or persons with personal knowledge of how the data was collected for the report. Without the Defendant being provided an opportunity to test the reliability of the data through cross-examination of a person or persons having personal knowledge of how the computer was able to provide data to tie an allegedly pornographic image to the Defendant, the information obtained through the CyberTip cannot be introduced.

The Court specifically rejects the State's contention that because the data is electronically generated, without the input of a human being, introduction of the document through Detective Petit would not deny the Defendant his right to confrontation. Two federal circuits appear to agree with the State's analysis, holding that an out-of-court statement generated automatically by a machine is not hearsay, in that to be considered hearsay the proffered evidence must be made by a declarant. By definition, a declarant must be a person. See United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005); Washington, 498 F.3d at 229. Here, the State claims that the information contained in the CyberTip was automatically generated and therefore is not a statement made by any declarant. The State analogizes the facts herein as similar to those before the Fourth Circuit in Washington. In Washington, the proffered evidence was a report of blood testing and the issue was the admissibility of tests generated by a gas chromatograph proving that

the defendant's blood contained evidence of drugs and alcohol. 498 F.3d at 229-30. In Washington, the Fourth Circuit Court of Appeals found that a blood test result indicating that PCP and alcohol was present in the defendant's system was not a statement of a person, but that of a chromatograph machine captured on a computer printout. Id. at 230. The chromatograph was operated by a lab technician and the defendant's argument was that the lab technician is required for cross-examination. The court found, however, that "there would be no value in cross-examining the lab technicians on their out-of-court statements . . . because they made no such statements. They would only be able to refer to the machine's printouts, which [the doctor] also had." Id. Here, the State argues that the information contained in the CyberTip is like the blood test reports in that it is merely an automatically-produced set of information from a machine, and that it is not an out-of-court statement subject to cross-examination.

The State also cites to the Tenth Circuit Court of Appeals in Hamilton, wherein the court found, in connection with a prosecution involving child pornography, that the "header information,"[1] even though automatically generated by a computer hosting the newsgroup, was not hearsay because it did not involve an out-of-court statement made by a declarant. Therefore, the information contained therein is not subject to the Confrontation Clause.

The State contends that the identifying information contained in Section A of the CyberTip is not hearsay and may be introduced without concern for the Defendant's right to confrontation. The First Circuit however has found to the contrary in connection with a child pornography trial. The court found that tip reports that were passed on to law enforcement authorities by a national reporting organization containing information provided to the national

[1] The "header information" referred to in Hamilton listed the person who posted the images, the person's screen name, the date the image was posted, and the person's IP address. Such information is nearly identical to the data referred to in the CyberTip.

organization by an internet service provider were testimonial statements since their primary purpose was to establish or prove past events potential to a later criminal prosecution. The court found that the admission of such reports without an opportunity to cross-examine the reports' authors violated the Confrontation Clause. Because the rationale of Crawford was inextricably tied to the reliability of data generated electronically, this Court accepts the rationale articulated by the First Circuit over that adopted by the Fourth and Tenth Circuits.

In this case, the data contained in the CyberTip constitutes the only evidence upon which the State relies to tie this Defendant to the images uploaded to his Cloud account which Microsoft reported to NCMEC. The reliability and authenticity of such data is essential to the State's burden of proof and should be tested in the "crucible of cross-examination."

Conclusion

Thus, this Court finds that once properly authenticated, a representative of the entity providing the inculpatory data must be made available for cross-examination by the Defendant. The admission of such report without the availability of such witness or witnesses violates the Defendant's constitutional right of confrontation. The parties will be expected to comport themselves at trial consistent with this in limine Decision.

RHODE ISLAND SUPERIOR COURT

Decision Addendum Sheet

TITLE OF CASE:	**State of Rhode Island v. Robert O'Brien**
CASE NO:	**K2-2015-0533A**
COURT:	**Kent County Superior Court**
DATE DECISION FILED:	**December 8, 2016**
JUSTICE/MAGISTRATE:	**Rubine, J.**
ATTORNEYS:	
For Plaintiff:	**Matthew L. LaMountain, Esq.** **Josh Owen, Esq.**
For Defendant:	**John E. MacDonald, Esq.**