IN THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
OF THE STATE OF FLORIDA IN AND FOR PASCO COUNTY

FILED IN OPEN COURT
THIS 14 DAY OF November, 2017
PAULA S. O'NEIL, CLERK & COMPTROLLER
PASCO COUNTY, FLORIDA
BY [redacted] D.C.

CRC14-05586CFAWS-04

STATE OF FLORIDA

v.

ADAM MATOS
SPN 00696506

: 1. MURDER IN THE FIRST DEGREE, Capital Felony
: 2. MURDER IN THE FIRST DEGREE, Capital Felony
: 3. MURDER IN THE FIRST DEGREE, Capital Felony
4. MURDER IN THE FIRST DEGREE, Capital Felony

STIPULATION

The parties, by and through their undersigned attorneys, hereby stipulate and agree as follows, alleviating the necessity for the State of Florida to require the testimony of the individual involved in the process of extracting data from the defendant's cellular telephone. This stipulation does not extend to the relevance of the evidence listed below.

The custodian of records (Custodian) for Apple, Inc. would testify with respect to the extraction process of retrieving data from the defendant's locked cellular telephone and each step taken in the extraction process. Apple legal and technical support staff responsible for reviewing and responding to legal process, and, in appropriate cases, recovering from Apple devices certain stored data are known as the extraction group. The Custodian would testify to the following:

First the extraction group checks the legal process (warrant) and evaluates if the process is appropriate/valid and that the device has verifiable identification numbers (i.e. IMEI/Serial number) that match those in the legal process. The extraction group then contacts the law enforcement agent and informs the agent that Apple can perform an extraction. The extraction group then obtains the device from the law enforcement agent and once the device is received, two persons from the extraction group review all of the relevant documents to ensure compliance. The extraction group then boots up the device using an internal iOS machine. A read only copy of certain information from the device is placed on storage media and that media is password protected before it is sent to the law enforcement agent in a sealed Federal Express box. The password for the encryption is separately emailed to the law enforcement agent. Apple devices can be protected by a user generated passcode, which is used to encrypt the data on the device which is a security measure, and because of this encryption the extraction process can only access a limited subset of the data that is on the device which is not encrypted with the user generated password. The data that is accessible to be extracted includes pictures, videos, voice recordings, SMS database, address book and recent call log. Before the extraction file is sent to the law enforcement agent, Apple runs a hash to ensure data integrity. Hash values can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value - the hash value - is produced that identifies the contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. The hash algorithm used in this case was SHA-256. After the extraction is performed and before the device and media are sent back to the law enforcement agent, both the device and the media are stored in a locked file cabinet in a locked office.

[redacted]

Joseph Lawhorne

Assistant State Attorney

[redacted]

Nicholas Michailos

Attorney for the Defendant

Adam

Defendant

Adam Matos