Catch Him With His Encryption Down: Counter-Encryption Techniques in Child Exploitation Investigations

Used throughout history to conceal sensitive information, encryption is the manipulation of data to prevent accurate interpretation by all but its intended recipients. Julius Caesar used a simple cipher to conceal his strategies, and Leonardo da Vinci wrote upside-down and backward in his notebooks, possibly to prevent others from learning his ideas. If you have logged in to your bank online, or used the Justice Department's remote connection software, you have also used encryption. Encryption can be used to protect data at rest that is in a container (like da Vinci's notebook or a hard disk), or data in motion (like the secure "https" web connection that your bank may provide, or the virtual private network offered by the Justice Department). Like many technologies, encryption technology can be used both for ethical and nefarious ends.

Encryption now appears in an increasing number of child pornography cases, where defendants use free-of-charge programs such as TrueCrypt or PGP (short for "Pretty Good Privacy") to encode their collections and their entire disks. This article offers (1) a brief overview of encryption and counter-encryption; (2) strategies that law-enforcement agents and prosecutors can employ when they suspect an offender is using encryption; and (3) discussion of a recent case, *In re Boucher*, that illustrates the difficult logistical and constitutional problems that can arise with encryption.

I. Overview of Encryption and Counter-Encryption: the Human Factor

Although good encryption can be hard to defeat, encryption is weakened by the fact that it is laborious and inconvenient. We have all seen doors with formidable locks that are left propped open. Thus, our recommendations for counter-encryption strategies center primarily on human factors -- human error and laziness in particular. Many encryption technologies require passwords. Of course, we also use passwords to log in to our computers, our email or instant messenger accounts (*e.g.*, Hotmail or MSN Messenger; Yahoo! or Yahoo! Messenger; Gmail or Gchat; ICQ), or online bank accounts. Passwords come with vulnerabilities: to remember them, people often write them down (and keep them near their computers) or use the same password again and again. A third vulnerability is that username and password information is easily recoverable using forensic techniques. For example, in one recent CEOS case, the forensic examiner was able to decrypt a defendant's PGP-encrypted folders after locating a set of user names and passwords that the defendant kept stored in unencrypted form within his Internet browser.

Furthermore, close observation of an offender's habits will often reveal occasions where the offender forgot or chose not to encrypt either the data in question, or the credentials needed to decrypt that data. Thus, human limitations– and human nature– often counteract and effectively nullify security technologies.

II. Addressing Encryption in Child Exploitation Investigations

The best way to handle an offender's use of encryption is to address it early on -- at the first stages of investigation and before indictment if at all possible. If offenders are discovered discussing their use of encryption, the prosecutor and agent should develop a strategy to maximize the chance of accessing the subjects' data when it is unencrypted. Using some of the below-mentioned techniques, the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team, along with CEOS's High Tech Investigative Unit, were recently successful in accessing the child pornography collection of a subject who was using TrueCrypt, which is "[f]ree open-source disk encryption software for Windows Vista/XP, Mac OS X, and Linux," to encrypt several of his hard drives.

If possible, develop a sense of when the offender uses his computer so that you have a chance of executing the search warrant while the offender is viewing child pornography and, necessarily, his encryption is disabled. The typical practice of executing search warrants at 6:30 a.m. or a similar hour works well for some offenders.

Consider using a ruse to cause the offender to leave his house quickly, before re-encrypting his disks. For example, obtaining a tow truck and pretending to repossess an offender's car has successfully drawn an offender out of his house so that his computer could be accessed by law enforcement in an unencrypted state.

Draft the search warrant affidavit with encryption in mind, and include language addressing the need to conduct a live forensic examination of the offender's media. This means that agents may need to examine media on scene, while it is still running, because pulling the plug will likely activate the encryption. Plan ahead for multiple agents to "baby-sit" the offender's media while the live examination and imaging completes. Today's offenders have large collections– numbering in the terabytes– that may take days to image.

Plan for a forensic examiner to respond to the search warrant scene in order to perform a computer forensic examination and analysis on the "live" evidence. As many agents have been trained to pull the device's plug before conducting forensics, be aware that, understandably, they may be uncomfortable with the idea of live forensics and counter-encryption procedures. They have been trained that a still-running computer presents forensic difficulties, as the device is not in a static state. However, methods exist to address this situation, and it is better to attempt to develop evidence with the subject's device still running than to power down the subject's computer and simultaneously power down your investigation. These methods include the preservation and collection of volatile data including the capture of RAM memory. Advanced forensic analysis can harvest passwords and encryption keys from the data captured in RAM memory, which typically is not saved to the hard drive. With the on-scene presence of the forensic examiner, the agent can rest assured that every technical step was taken to preserve and collect data of evidentiary value. *See generally*, Marcus K. Rogers, *et al.*, *Computer Forensics Field Triage Process Model*, Journal of Digital Forensics, Security and Law (2006).

If all of this sounds like a lot of bad news and hard work, then there is some good news as well: the most widely-used forensic software packages– such as FTK and EnCase– have robust counter-encryption functionality built in, and these packages can be used to perform live forensic capture. Thus, while additional training may be needed for counter-encryption and live forensics, it should not be necessary for agents to buy new software or equipment.

III. Compelling Evidence - May an Offender be Required to Decrypt?

In addition to those instances where an investigator or forensic examiner discovers the encryption key or password during the course of a lawful search, in some cases an offender may voluntarily provide the key or password to his encrypted devices. But what is a prosecutor to do in other cases -- may an offender be compelled to provide his key or password?

The issues and questions quickly become complicated, and a universal answer not easily discerned. *See generally*, *Compelling the Production of Encryption Keys and Passwords*, CHILD EXPLOITATION AND OBSCENITY SEC. Q., Oct. 2004; *see also United States v. Pearson*, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006). A recent case illustrates some of the constitutional complexities that encryption can create and demonstrates how the particular facts of the case, including what is being compelled, may be the decisive factor.

In re Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) involved a defendant who entered Vermont from Canada. (Note that this opinion is under seal, but remains available on Westlaw, apparently due to a brief, inadvertent publication of the opinion on PACER.) Customs officers found a laptop in the back of defendant's car and examined its contents, finding several thousand image files, some with file names indicative of pornography. An officer asked defendant if any of the image files on the laptop contained child pornography, and defendant said he was uncertain. The officers continued to examine the laptop, and noticed several file names that appeared to reference child pornography. Another agent with specialized experience was called in and found a file titled "2yo getting raped during diaper change." This agent was unable to open this file, but determined that it had been opened on December 11, 2006. The agent turned back to the computer and found thousands of images of adult pornography and animation depicting adult and child pornography.

The defendant waived his *Miranda* rights and agreed to speak to the agent. Defendant stated that he downloaded pornography, and sometimes unknowingly downloaded child pornography. Defendant told the agent that he kept his pornography in a part of his hard drive called Drive Z. The agent began navigating Drive Z, with defendant in the room, and defendant grew uncomfortable while the agent found numerous adult pornography files, and one apparent child pornography file. The agent again asked defendant whether he had any similar files on his laptop, and defendant said he usually deleted files that he found to contain child pornography.

The agent then asked defendant to leave the room, and continued to examine Drive Z. The agent found more child pornography images, and arrested defendant. Finally, the agent seized defendant's laptop and shut it down. Twelve days later, another agent attempted to begin a forensic analysis of the laptop, but discovered that it had re-encrypted. All subsequent attempts to view the images within Drive Z were unsuccessful, and the agents were unable to learn the password.

The prosecution obtained a grand jury subpoena ordering defendant to produce his password. Defendant moved to quash the subpoena, and at a hearing on the motion, the government suggested that defendant could enter the password into the computer without it being recorded by the government or the grand jury. The government further suggested that, in order to avoid Fifth Amendment issues, the Court could order that the act of using the password not be used against defendant.

The magistrate granted defendant's motion to quash the subpoena, holding that the act of entering the password was testimonial in nature, such that the Fifth Amendment privilege against self-incrimination applied to it. *In re Boucher*, 2007 WL 4246473 (Nov. 29, 2007). The magistrate reasoned that providing a password conveyed the contents of one's mind, in a way that turning over a strongbox key, or submitting to blood or fingerprint analysis did not.

The magistrate further held that even if defendant merely entered his password into the computer without it being recorded, the testimonial nature of this act would persist. The magistrate similarly rejected the government's suggestion that the Court order that defendant's use of the password not be used against him, citing *United States v. Hubbell*, 530 U.S. 27 (2000). Essentially, the Fifth Amendment protection had to extend not only to the act of production itself, but any derivative use as well.

The magistrate's opinion finally dealt with the government's argument that the information gained through the entry of the password was a "foregone conclusion," such that no privilege applied. This argument was based on a Second Circuit case holding that the privilege against self-incrimination did not apply to an act of production if the existence and location of the subpoenaed evidence was known to the government and the production would not "implicitly authenticate" the evidence. *See In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992*, 1 F.3d 87, 93 (2d Cir. 1993). The magistrate reasoned that the subpoena either compelled production of the password itself, or alternatively the contents of Drive Z, and that, either way, the foregone conclusion doctrine did not apply.

The government appealed the magistrate's ruling to the District Court, which reversed. The District Court held that requiring defendant to produce an unencrypted version of his Z drive would not constitute compelled testimonial communication. This analysis turned on the District Court's assertions that the government already knew of the existence and location of Drive Z and its files, and defendant's act of production of the drive was not needed to authenticate it. The District Court barred the government from using defendant's act of production to authenticate the unencrypted Z drive or its contents.

Boucher raises a number of novel and interesting Fifth Amendment issues, but also begs a more practical question: what would have happened if the agent, instead of shutting down the laptop, had commenced a live forensic capture? The agent could have recovered a forensic copy of the contents of Drive Z, obviating the constitutional arguments that ensued. Although we still await the ultimate resolution of the Fifth Amendment questions raised by *Boucher*, one message from the case is already clear: in cases involving encryption, the employment of on-scene live forensics may help avoid constitutional trouble down the road. }

Biographical data is any that can be gathered about the individual who created the passwords being recovered. This information could be any of the following: names, addresses, cities, states, zip codes, countries, phone numbers, dates, numbers, words, and even phrases. These data elements are broken up into their constituent parts and then recombined to produce candidate passwords.

Sample Biographical Dictionary

Name	Johnathan Bridbord
Address	1400 New York Ave, N.W.
City	Washington
State	D.C.
ZIP Code	20530
Country	USA
Phone Number	202-514-5593
Fax Number	202-514-1793
Email address	Johnathan.Bridbord@usdoj.gov
Date of Birth	January 1, 1970
Anniversary Date	July 4, 1776
Social Security Number	123-45-6789
Word	supercalafragalistic
Phrase	Oh, Danny boy The pipes, the pipes are calling From glen to glen And down the mountainside
Favorite Movie	The Godfather
Favorite Team	Yankees