



## **WHITE PAPER**

### **"ENCRYPTION AND COMPELLED DECRYPTION"**

Can the government force you to decrypt encrypted files on your laptop computer so they can use those files to send you to jail? On February 19, 2009 United States District Judge William Sessions in Vermont ruled that they could. In fact, the Court found that the defendant had no privilege against self-incrimination with respect to the act of decrypting the files.

On December 17, 2006 Sebastian Boucher and his dad drove back to the United States in Derby Line Vermont after a brief trip to Canada. US Immigrations and Customs (ICE) agents saw Boucher's laptop computer in the back seat of the car, seized it, opened it, and examined its contents as a "border search." They found 40,000 images, some of which had file names that indicated they were pornographic, and some of which may – based on the file names alone – have been child pornography. The ICE agent had Boucher show him files on the computer, and believed that he might have child pornography, which is contraband and illegal to knowingly possess or import into the United States. However, these files were on Boucher's "Z" drive. Once the machine was shut down at the border (after Boucher was arrested) the drive was encrypted. The question for the court was not the legality of the border search, or Boucher's consent to the initial examination, but whether they could now force him to decrypt the drive.

It has long been the law in the United States that the incriminating contents of voluntarily created documents or files are not protected under the self-incrimination provisions of the Fifth Amendment. Thus, if you decide to keep a record of your criminal activities on paper, the government can force you to pony that up, just as they can force you to turn over the murder weapon hidden under the bed, or your tax records and receipts that show fraud. While the documents are incriminating, and you are being "compelled" to produce them, you weren't compelled to create them – or so the courts reason. However, there is an exception to this general rule. Sometimes the mere act of turning something over has "testimonial" qualities. For example, responding to a subpoena that calls for the production of "all guns you used to kill Jane Doe" would inevitably call on you to incriminate yourself by the act of production. Where your possession or custody of a document or record is in issue (or your knowledge of its presence or existence) the so-called "act of production" can be incriminating and ordinarily can't be compelled unless the government agrees never to use the fact that you produced the thing, or information derived from the fact that you produced in any criminal case against you. Again what is immunized is just the act of production, not the contents of the file.

In Boucher's case, the government agreed not to use his act of decryption against him. They already could establish that Boucher admitted that the computer was his, and that he had created the Z drive. In fact, Boucher admitted to the existence of porn on the machine, and to the fact that, in the course of

downloading porn, he may have inadvertently downloaded child porn, which he contended he “immediately deleted.” The district court noted that, technically Boucher was not being asked for his decryption key. He wasn’t being compelled to “testify” about his PGP password. Rather, we was being compelled to provide a decrypted copy of the Z drive. Thus, he wasn’t being compelled to “testify.” While ordering the government not to use Boucher’s act of production to authenticate the unencrypted Z drive or its contents, the Court ordered Boucher to decrypt the drive itself. This case represents the first time the government has compelled a target to decrypt a file to be used in a criminal case against them. In a previous case, *United States v. Scarfo*, Criminal No. 00-404 (D.N.J. 2001) the government obtained a court order to deploy a key-logger onto Scarfo’s computer to capture his PGP key, which it later used to read the files on his computer. But Scarfo wasn’t forced to give up his key or to decrypt his data. It is also important to note that, while the government seized Boucher’s computer because it had at least reasonable suspicion that it contained incriminating evidence or contraband, under current law it is likely that they would need no such evidence to compel someone to decrypt their files. A grand jury – which is what the government used in this case – has the right to what the court has termed “everyman’s evidence.” This applies whether you are a target of an investigation, a victim, a witness or a passerby. As long as there is an investigation (and now even if the investigation involved gathering intelligence and not merely law enforcement) the government may convene a grand jury, subpoena your electronic records, and compel you to decrypt them. In civil cases, private litigants would also be able to compel production and decryption of otherwise unprivileged records. Thus, while encryption may provide technical protection against unauthorized access, it provides little legal protection. So what if you use the “Steve Martin” defense when asked to provide you decryption key, simply saying, “I forgot?” It is likely that an unbelieving court will be happy to jog your memory by holding you in contempt of court and fining or incarcerating you until your memory is sufficiently jogged. We can anticipate many more cases involving encrypted files and records, but it is likely that Judge Sessions’ ruling will ultimately be the law of the land.