Legal Update

December 2017

Issue: Can the court issue an order directing a defendant to supply his personal identifying number (PIN) access code into his smart phone and issue a contempt order for failing to comply?

In the Matter of a Grand Jury Investigation, Mass. App. Ct. NO. 16-P-215, (2017): A Middlesex County grand jury requested that an assistant district attorney seek an order from a Superior Court judge as part of an ongoing investigation of an assault and battery on two children. The Commonwealth filed a motion ordering the petitioner to produce the PIN code and any other electronic key or password required for the iPhone that was seized after the issuance of a search warrant.

The motion, the proposed order, and two documents were filed in court under seal and served on the petitioner's attorney. Two documents were not provided to the petitioner's counsel. The first document was a statement demonstrating the petitioner's ownership and control of the iPhone. The second document was an affidavit of the assistant district attorney, which summarized the evidence before the grand jury; appended to the affidavit was a transcript of the grand jury proceedings. After a hearing, the motion was allowed as well as an order entered detailing the protocol by which the petitioner would enter the PIN code so that the search warrant could be executed. When the petitioner refused to comply with the order, the Commonwealth filed a petition for civil contempt. The petitioner was ordered held in custody until he purged the contempt by complying with the order. A stay of execution of the judgment was allowed by agreement.

For specific guidance on the application of these cases or any law, please consult with your supervisor or your department's legal advisor or prosecutor.

Conclusion: The Appeals Court concluded that the motion and subsequent order compelling the petitioner to produce his PIN for the Commonwealth to access the phone was not a violation of the petitioner's Fifth Amendment Rights. The issue the Appeals Court considered was whether ordering the petitioner to supply his PIN qualified as testimonial evidence and violated his Fifth Amendment Rights.

First the Appeals Court considered what qualifies as testimonial evidence. The Supreme Court has previously summarized that "while the Fifth Amendment privilege typically applies to oral or written statements that are deemed to be testimonial, the act of producing evidence demanded by the government may have communicative aspects that would render the Fifth Amendment applicable. Whether an act of production is testimonial depends on whether the government compels the individual to disclose the contents of his own mind to explicitly or implicitly communicate some statement of fact. More particularly, the act of complying with the government's demand could constitute a testimonial communication where it is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence."

Courts have also previously found that compelled evidence may not be regarded as testimonial if the information provided qualifies as a foregone conclusion. ***Id*** at 522. The forgone conclusion exception to the Fifth Amendment privilege against self-incrimination provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, and therefore adds little or nothing to the sum total of the Government's information. The Commonwealth bears the burden of proving the foregone conclusion exception. First the government must show" its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence." ***Ibid.***

When the government independently and with specificity established the authenticity, existence, and possession of the compelled information, the forgone conclusion exception may apply. ***Gelfgatt***, supra at 522. In ***Gelfgatt***, the Commonwealth possessed "detailed evidence" of fraudulent mortgages linked to a financial services company. 468 Mass. at 523. When the defendant was arrested, he told police that he worked for the financial services company and had communications with the company contained on his home computers, which he had encrypted and only he could decrypt. ***Id***. at 517. The court in ***Gelfgatt*** acknowledged that the defendant's admission of entering an encryption key into his computers, demonstrated that he had ownership and control of the computers. However, the court found that "the factual statements that would be conveyed" were a "foregone conclusion," ***Id***. at 523, because "the defendant's act of decryption would not communicate facts beyond what the defendant already admitted to investigators." ***Id***. at 519.

For specific guidance on the application of these cases or any law, please consult with your supervisor or your department's legal advisor or prosecutor.

Here, ordering the petitioner to enter the correct PIN code, only communicates evidence that is merely a foregone conclusion and "adds little or nothing to the sum total of the Government's information." ***Id.*** at 522, quoting from ***Fisher***, supra. The Commonwealth was not required to show that it knew the specific content of the iPhone, but it did need to demonstrate knowledge of the existence and the location of the content. Id. at 523, citing ***United States v. Fricosu***, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) ("Fifth Amendment not implicated by requiring production of unencrypted contents of computer where government knew of existence and location of files, although not specific content of documents, and knew of defendant's custody or control of computer").

Additionally, the Commonwealth demonstrated sufficient knowledge to show that the factual statements that the petitioner's act of entering his PIN code would convey are foregone conclusions. The Commonwealth already knew that the iPhone contained files that were relevant to its investigation based, on information provided by the petitioner. The PIN code was necessary to access the iPhone, and it was clear that the petitioner possessed and controlled the iPhone, and knew the PIN code and to access the phone. The Commonwealth established independently and with specificity the authenticity, existence, and possession of the compelled information. The order does not require the petitioner to communicate information that would fall within constitutional self-incrimination protection. The affidavit in support of the search warrant application established that the Commonwealth had probable cause to believe that the iPhone contained evidence of the crimes that are the subject of the grand jury investigation. The order simply allows execution of that warrant.

Lastly, with regard to the contempt charge, the Appeals Court held that that the judge did not abuse her discretion by allowing the civil contempt order. To constitute civil contempt there must be a clear and undoubted disobedience of a clear and unequivocal command." ***Manchester v. Department of Envtl. Quality Engr***., 381 Mass. 208, 212 (1980). Here the petitioner was in civil contempt for failing to provide the PIN code to access his Iphone as he was ordered to do. See ***Eldim, Inc. v. Mullen,*** 47 Mass. App. Ct. 125, 129 (1999).

For specific guidance on the application of these cases or any law, please consult with your supervisor or your department's legal advisor or prosecutor.