12-2014

Encryption and Incrimination: The Evolving States of Encrypted Drives

Shannon M. Oltmann
University of Kentucky, shannon.oltmann@uky.edu

Encryption and Incrimination: The Evolving States of Encrypted Drives

Encryption and Incrimination: The Evolving Status of Encrypted Drives

by Shannon M. Oltmann

EDITOR'S SUMMARY

Individuals use encryption to safeguard many valid and legal applications but also to hide illegal activity. Several legal cases have drawn the limits of self-incrimination under the Fifth Amendment regarding providing passwords to access illegal information content, such as child pornography. The cases illustrate that certain knowledge of evidence amounts to a compelling need for access and that a subpoena for hard drive contents is more likely to succeed than requiring a witness to provide a password. Since known documents are not legally protected and biometric data can be compelled as evidence, there is no reason that known digital documents, biometric passwords, and by extension, alphanumeric passwords should not be compelled. Considering precedent and legal doctrine, individuals should resist giving law enforcement any passwords and be wary of sharing them. The question of encryption in criminal cases is under scrutiny and warrants citizens' concern.

KEYWORDS

encryption

information access

electronic documents

law enforcement

Shannon M. Oltmann is an assistant professor in the School of Library & Information Science at the University of Kentucky. She can be reached at shannon.oltmann<at>uky.edu.stacy<at>greenfx.net.

Encrypted computer files and drives are becoming increasingly commonplace, with multiple free or inexpensive applications allowing individuals with divergent technical skills to encrypt files with ease. From a legal standpoint, "...both the promise and peril of encryption arise from its very effectiveness – properly implemented, a strong encryption regime provides near absolute security" [1, p. 599].

There are many reasons one might have encrypted files or an encrypted drive. Encryption is routinely used to secure RFID tags and transmission of payment information and medical records. Although there are numerous institutional uses of encryption, this article focuses more on individual use. There are also many resources for learning more about encryption. See, for example, [2], [3], [4].

In individual use, one could be protecting private information (such as legal records, financial information or passwords), intellectual property (trade secrets, patents and inventions), legally protected information (records protected by the Health Insurance Affordability and Accountability Act – HIPAA – or the Family Educational Rights and Privacy Act – FERPA) or confidential information (sensitive academic research, media informants). One may also encrypt data out of an abundance of caution or privacy. Of course, people often encrypt data that would be probative of illegal activity (including child pornography, fraud, pirated media and extortion).

This latter use remains a relatively untested area legally. In the past decade, only a handful of cases have addressed the convoluted issues of encrypted data and self-incrimination, with differing outcomes, as illustrated here:

United States v. Pearson (2006): Pearson faced multiple charges related to child pornography. While out on bail, he re-acquired the images in question and then encrypted those files. The FBI subpoenaed Pearson's passwords, but he refused to incriminate himself. (Note: Both legal analysis and criminal courts have been unclear in their use of *password*, which has been used frequently as a synonym for *decryption key*. This article follows this practice.) The case was further complicated because the hardware belonged to Pearson's father, an attorney, who belatedly claimed attorney-client privilege. Eventually, Pearson pled guilty to some of the charges.

In re Boucher (2009): Boucher entered the United States from Canada. A border agent examined Boucher's computer and found child pornography after Boucher supplied the password. The agent then shut down the computer and arrested Boucher. Shutting down the computer triggered the encryption again, and prosecutors could no longer see or find the illegal images. Boucher was ordered by the courts to supply the password, but he invoked his Fifth Amendment privilege. The courts subsequently ruled he had to supply a decrypted copy of the drive's contents.

United States v. Kirschner (2010): Kirschner was indicted for child pornography charges, and the government subpoenaed his encryption key to gain further evidence from his encrypted drive. In this case, the judge determined that requiring a defendant to supply his password would violate his right against self-incrimination.

Commonwealth v. Hurst (2011): Hurst was charged with offenses related to inappropriate sexual relations with a minor. Police suspected incriminating evidence was on Hurst's cellphone, but he refused to supply the password. Before this case reached the court system, Hurst's wife supplied the password, and Hurst himself pled guilty.

United States v. Doe (2012): Doe was charged with child pornography. He refused to supply his decryption key and was found in contempt of court, then jailed. A judge then ruled that supplying his decryption key would be tantamount to self-incrimination, so Doe did not have to supply it.

United States v. Fricosu (2012): Fricosu was indicted for mortgage and real estate fraud. She refused to surrender the password (at one point saying she forgot the password) to encrypted files that, the government believed, would incriminate her. The court ordered her to supply a decrypted version of the hard drive, rather than her password. Subsequently, a co-defendant supplied the needed passwords.

Summary of Protections Against Self-Incrimination

At first glance, these cases do not provide consistent precedent. However, there are a few factors that were important in nearly all of these cases. To better understand these rulings, we need to review certain legal concepts and doctrines.

The relevant portion of the Fifth Amendment states that an individual shall not "be compelled in any criminal case to be a witness against himself." To claim the protection of the Fifth Amendment, a defendant "must demonstrate that (1) he has been compelled (2) to produce testimony (3) that is incriminating" [5, p. 1125]. This statement neatly summarizes the complex, evolving legal doctrines surrounding self-incrimination. According to the first point, a defendant cannot be compelled to create new documents, but if the documents or information that the government seeks already exist, then requiring a defendant to produce them is generally not considered incriminating (though there are exceptions to this rationale; see [6], [1]). In each of the aforementioned cases, the information in question was already present and had been voluntarily created, "which rendered their content exempt from Fifth Amendment protection; thus, the entire analysis in each opinion considered whether the *act of production* would invoke the [self-incrimination] privilege" [1] (emphasis added).

For the purposes of this legal doctrine, "testimonial evidence" is explained as "a communication of information from the [defendant's] memory or knowledge" [7]. Providing a key to a locked box or blood for a DNA test are thus not considered self-incriminating "testimony" and can be forced. Finally, *incriminating* simply means that the compelled testimony is likely to support conviction.

In addition, "the government must prove the existence and location of the subpoenaed documents and possess independent evidence, other than compliance with the court order, for authenticating them" [1, p. 581]. In

other words, law enforcement cannot simply go on a fishing expedition, hoping to turn up data that will be evidentiary [8]. They must be able to demonstrate the existence and likely location of specific documents.

Analysis of Recent Cases

From this summary of relevant legal doctrine, we can tease apart some of the differences and contradictions in the preceding cases. Law enforcement saw evidence of criminal wrongdoing in the Pearson, Boucher, Hurst and Fricosu cases. Both Pearson and Boucher voluntarily agreed to let law enforcement search their computers; during those searches, the officers saw evidence. It was only after the initial search that the question of encryption became relevant. In these cases, because the defendants had "permitted investigators to see at least some" of the evidence, this "sufficed to render the existence of all the illegal files a 'foregone conclusion'" rather than testimonial evidence [8, p. 544]. Hurst had sent inappropriate messages to a minor, which were visible on the minor's phone. While the police sought confirmation of the transmission by searching Hurst's phone, they had sufficient evidence without that step. In the Fricosu case, police had recorded conversations between the defendant and her husband (a co-defendant) that revealed the existence and content of the sought-after documents.

In contrast, law enforcement in the Kirschner and Doe cases did not have prior evidence that illegal content was on their computers. In these cases, officers had suspicion of wrongdoing and were relying on the revelation of decryption keys to investigate and uncover evidence. The court in Kirschner determined that sharing the key "would be testimonial because it would demonstrate knowledge of the password and access to the underlying computer files …providing the password would reveal the contents of an arrestee's mind by recalling the password" [5, pp. 1171-1172], [6]. Simply put, because the password was not written down (or already known to law enforcement) in Kirschner and Doe, and it existed only in their minds, compelling a defendant to reveal it would be self-incriminating testimony.

A final difference among some of the cases lies in the subpoenaed request: in some cases, law enforcement wanted the defendant to provide an unencrypted copy of the hard drive, while in other cases they asked for the defendant's password, which would then be used to decrypt the data [6]. In Pearson and Hurst, officials wanted the passwords but had sufficient evidence to convict without it. Boucher was first ordered to give his password, then to supply a decrypted version of the drive. Fricosu and Hurst were likewise first ordered to supply passwords, but law enforcement received assistance from their spouses in deciphering the passwords, so defendant cooperation was not necessary. In both Kirschner and Doe, officials were requesting the password, and the subpoena was quashed due to Fifth Amendment protections.

If law enforcement can describe the existence and location of evidence, they have a stronger case for requiring access; however, if they cannot demonstrate prior knowledge of the likely data, separate from a compelled revelation from a defendant, then law enforcement has a weaker position.

Some tentative conclusions can be drawn based on these cases. One of the most important elements is whether the existence of evidence is a "foregone conclusion," as it was in Pearson and Boucher. If law enforcement can describe the existence and location of evidence, they have a stronger case for requiring access; however, if they cannot demonstrate prior knowledge of the likely data, separate from a compelled revelation from a defendant, then law enforcement has a weaker position. Second, it appears that subpoenaing the contents of the computer drives, rather than the key to decrypt them, is more likely to be successful. Recall that the courts quashed the subpoenas for passwords from Kirschner and Doe, while Boucher was ordered to surrender an unencrypted drive.

The Problem with Passwords

These cases, while relatively few, do seem to gradually build some points of consensus. However, scholars are split about the wisdom of this consensus and whether the cases so far are a solid foundation for legal precedent. In particular, the two recent cases (Kirschner and Doe) that quashed subpoenas for passwords are more problematic than they might at first appear.

Protecting a password or encryption key based on self-incrimination does not seem to be a legally consistent argument and is likely to be clarified and overturned as these or similar cases work their way up the court system.

Because courts can usually compel defendants to produce already-existing documents, even if they are private, "it makes little sense to deprive the grand jury of relevant evidence, after the encoding, merely because the author has transformed it into an even more private form" [1, p. 604]. A defendant may be compelled to produce business documents, a diary or pornographic images, even if those documents substantiate charges against him, because the courts have held that the Fifth Amendment does not protect already existing documents (unless the act of production itself would constitute testimony). This doctrine holds even if the documents are, say, sealed in an envelope or locked in a safe. Thus, it is counterintuitive for data stored on a computer to enjoy additional protection merely because it is protected by a password or hidden through encryption. Ungberg (2009) notes that "sometimes a single password shields thousands of documents that would otherwise be subject to government seizure with a simple search warrant" [8, p. 554].

In addition, there is well-established precedent that biometric data (whether it be fingerprints, DNA samples or saliva) can be compelled. It seems illogical that a biometric password could be legally subpoenaed, but an alphanumeric one could not [6]. Thus, protecting a password or encryption key based on self-incrimination does not seem to be a legally consistent argument and is likely to be clarified and overturned as these or similar cases work their way up the court system.

Implications for Encryption Users

One lesson to be learned from these recent cases is to resist volunteering one's password or access to one's computer. Both Pearson and Boucher initially allowed law enforcement to examine their hard drives, which was a key reason that courts subsequently determined they had no right to refuse further examination. Indeed, the Electronic Frontier Foundation (EFF) offers advice if law enforcement seizes your computer: "…first off, don't give them your password during the search – you have the right to remain silent, so use it. Since they can't search your encrypted files without your help, you've got leverage that most search targets never have" [9]. The next step, according to EFF, should be calling a lawyer.

A second lesson is to be cautious when sharing passwords. Both Hurst and Fricosu had their passwords revealed by their spouses. Hurst's wife did not want to protect him, and Fricosu's husband was a co-defendant who likely received a lighter sentence. However, either spouse could have been charged with contempt of court for not revealing the passwords – and it would be likely to happen to other close associates. Law enforcement may very well use this as a threat to compel others to share their relevant information.

If the defendant chooses to not reveal the password, as in Doe's case, he is likely to be charged with contempt. For some defendants, contempt of court is a preferable charge to the ones they are likely to face. Receiving child pornography, for example, typically has a minimum sentence of five years and requires registry on a sex offender list, which together make contempt of court charges seem attractive. However, there are other cases in which individuals may not want to reveal encryption keys and instead choose contempt of court: journalists protecting sources, businesses protecting trade secrets, intelligence operatives protecting strategic information and so on.

Some scholars recognize that a contempt of court charge may not persuade individuals to reveal their passwords or decrypt their hard drives. In Pearson, the government tried suggesting that having a very large encrypted drive was itself suspicious and indicative of illegal activity, but this argument was rendered moot once Pearson cooperated [1]. Law-abiding citizens who encrypt files – for whatever purpose – should take note. In a separate yet related move, Larkin suggests that the government should be able to use a "missing evidence instruction" when a defendant refuses to decrypt. According to this approach, "the court may instruct the jury to draw an inference that the missing evidence or testimony would have been unfavorable" [6, p. 276l]. As Larkin notes, missing evidence instructions

tend to strongly affect juries. While this instruction seems reasonable when defendants are accused of child pornography, in other situations its application is more problematic. Should a presumption of "unfavorable" content be made in cases of journalists protecting sources or businesses protecting trade secrets? Again, encryption can be used to protect both legal and illegal files to safeguard legal, illegal or questionable activities. The courts are still working out the appropriate approach to individuals who use encryption to facilitate breaking the law; academic analysis and reflection is still relatively sparse.

There has been even less work to-date considering legal users of encryption and how they might fare in the criminal court system. With the recent revelations about the depth and breadth of National Security Agency (NSA) surveillance, increased caution and concern seem reasonable, particularly since the NSA has stated that it keeps all intercepted, encrypted communication until it can be decrypted and analyzed – which, by the very nature of modern encryption, is an indefinitely long period of time [10]. For decades, there has been a struggle between users who want to encrypt files and the government which wants access to those files. The legal realm has yet to reach a consensus on the appropriate way to facilitate government access or to address government suspicions about legal and encrypted files. ■

Resources Mentioned in the Article

[1] McGregor, N.K. (2010). The weak protection of strong encryption: Passwords, privacy, and Fifth Amendment privilege. *Vanderbilt Journal of Entertainment & Technology Law, 12*, 581-609.

[2] Boneh, D., Sahai, A., & Waters, B. (2012). Functional encryption: A new vision for public-key cryptography. *Communications of the ACM, 55*(11), 56-64.

[3 Mathur, A. (2012). A research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. *International Journal on Computer Science & Engineering, 4*(9), 1650-1657.

[4] Olangunju, A., & Soenneker, J. (2012). A real-time performance analysis model for cryptographic protocols. *Journal of Systemics, Cybernetics, & Informatics, 10*(6), 68-75.

[5] Gershowitz, A.M. (2011). Password protected? Can a password save your cell phone from a search incident to arrest? *Iowa Law Review, 96*, 1125-1175.

[6] Larkin, J.E.D. (2012). Compelled production of encrypted data. *Vanderbilt Journal of Entertainment & Technology Law, 14*, 253-278.

[7] Dripps, D. (2005). Self-incrimination. In *Heritage Guide to the Constitution* (D. Forte & M. Spalding, eds.), pp. 335-335.

[8] Ungberg, A.J. (2009). Protecting privacy through a responsible decryption policy. *Harvard Journal of Law and Technology, 22*(2), 537-558.

[9] EFF. (n.d.) Encrypt your data. Surveillance Self-Defense Project. Retrieved October 12, 2013, from http://ssd.eff.org/your-computer/protect/encrypt

[10] Masnick, M. (June 21, 2013). NSA: If your data is encrypted, you might be evil, so we'll keep it until we're sure. *Techdirt*. Retrieved October 12, 2013, from www.techdirt.com/articles/20130620/15390323549/nsa-has-convinced-fisa-court-that-if-your-data-is-encrypted-you-might-be-terrorist-so-itll-hang-onto-your-data.shtml