WINTER 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With increasing encryption usage and the recent news of the government requesting Apple to provide "backdoor" access to iPhones, we chose to theme this E-Newsletter on the impact data encryption has on attorneys, litigation support professionals and investigators.

ENCRYPTION AND LEGAL DISCOVERY: WHOSE SIDE ARE YOU ON, ANYHOW?

In the United States, the absence of mandatory key discovery laws regulating the production of cryptographic keys and data encryption and rules of legal discovery continue to stand in apparent opposition as the speed of development outpaces the establishment of judicial precedent. Encryption users embrace increased protection of information, while holders of valid subpoenas are frustrated by difficulties with decryption, and find themselves turning back to the courts for further guidance and assistance. The sun may have set on the days when the bulk of document production meant cartons of paper files delivered by tractor-trailer; however, we appear to be well into a new day of electronic challenges. Whether encryption is a benefit or hindrance in legal discovery is a matter of perspective.

Encryption: Friend or Frenemy?

Encryption is the process or practice by which data is made unintelligible without a key to reverse and render readable the scrambled or hidden information. The role of encryption typically is to protect both author and potential recipient from prying eyes by limiting access to those who have the key, and scrambling information for secure exchange and storage. The benefit of encryption is security. Securely storing and transmitting data isn't just good practice when handling sensitive information; it's often a contractual obligation or regulatory requirement in many industries, such as banking and medical.

While banking online without the fear of broadcasting account details is an easy nod to the benefit of encryption, the same technology is employed to conduct illegal transactions surreptitiously. Therein, lies the frustration for law enforcement. February 26, 2016, is the deadline for Apple, Inc. ("Apple") to respond to a federal court's order that Apple assist the FBI to "bypass or disable" the security feature on the iPhone used by one of the shooters in the December 2015 San Bernardino attack. While technically the order does not require Apple to

decrypt the information on the phone, Apple CEO Tim Cook wrote in defense of the company's refusal to comply, "The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe." While the Court awaits Apple's response, debate over the FBI's request rages.

In October 2015, the director of the FBI announced at a Senate committee hearing that President Obama's administration would not take action to force companies to decrypt communications. This announcement concurs with the bulk of case law that previously denied government and law enforcement agencies motions to compel the production of encryption keys or to decrypt data. As the first case to address the encryption key issue, *In re Boucher* has been touted as a litmus test with regard to how far the Fifth Amendment protection against self-incrimination extends in the face of encryption technology. In a motion to quash a subpoena *In re Boucher*, the Court found that the government was not entitled to the defendant's encryption key despite US Customs having already discovered child pornography on the subject laptop.

In September 2015, in *Securities and Exchange Commission v. Bonan Huang, et al.,* the US District Court ruled that defendants could not be compelled to provide access to, and by extension decryption of, encrypted data on company issued cell phones. The court ruled that the SEC did not have the right to request decryption of data in order for the SEC to determine if any encrypted documents on said cell phones would be subject to a previously issued document request. This case relied on the defendants' Fifth Amendment Right, which the Court determined was properly asserted.

Although the bulk of case law currently comes down on the side of protecting encryption key privacy, that's not to say the courts have unanimously declared encrypted data off-limits in discovery. In an employment law matter, *Enargy Power Co. v. Xiaolong Wang*, 2013 WL 6234625 (D. Mass. 2013), a former employee was required to facilitate decryption of allegedly stolen work product for his former employer.

Discovery: Cracking the Shell Game?

The purpose of discovery is to locate relevant information, be it electronic or otherwise, and includes metadata, which provides information regarding the generation of data. For parties involved in legal discovery, encryption is a tenacious issue. Electronically stored information holders subject to discovery proceedings may wish to look for a simple refusal, such as lack of possession of the public key to the encrypted information. In a 2014 Federal case, *Cochran vs Caldera Medical, Inc.,* the court found that the respondent's inability to access the encrypted data relieved the respondent of their obligation to produce the data at that time. However, simply because key release isn't compelled, doesn't mean the data is irretrievable.

E-discovery firms have successfully employed various methods of key retrieval. With the rise in employers condoning the use of employee-owned cellphones and laptops for work, employers can easily claim they don't have access to the encrypted data on employees' personal technology. Since employees can be subpoenaed for information without being a named party to the action, this approach isn't foolproof. Additionally, Courts have required respondents to engage e-discovery firms to "break" the encryption resident on servers and non-network storage devices in order to comply with discovery. These rulings thwart the idea that by placing the time and cost of breaking the encryption on the requestor, the respondent can successfully claim ignorance of the key as the electronic equivalent of shifting the shells to hide the walnut.

Innovations in encryption technology won't stop coming any time soon. As long as the need to protect data exists, and encryption weaknesses are found, development of more effective data protection will proceed at a rapid pace. Courts and legislatures have a history of taking time to

mull over issues before reaching consensus, and mandatory key disclosure is no exception. Apple may have limited time to respond to the court order, however, the ultimate outcome of the battle between Apple and the FBI will undoubtedly have long-lasting ramifications. E-discovery firms bridge the gap between encryption and discovery by providing the essential services to decrypt and retrieve relevant information. As long as there is electronically stored information to be retrieved, e-discovery will be the fastest way to do it. Whether e-discovery has you jumping for joy or not may depend on which side of the encryption fence you reside.

If you would like to be considered as a future Guest Contributor to a Digital Mountain E-Newsletter, please provide a biography and a description of the proposed article to marketing@digitalmountain.com**.**

UPCOMING INDUSTRY EVENTS

February-March 2016
RSA Conference, San Francisco: February 29 - March 4

March 2016
Fifth Annual ASU-Arkfeld
eDiscovery and Digital Evidence Conference, Tempe: March 9-11

ABA Techshow 2016 Conference and Expo, Chicago: March 17-19

April 2016
The Masters Conference, San Francisco: April 19

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: