SPRING 2021 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss mobile device trends for legal and security, including malware, authentication, and legislation around backdoors to end-to-end encryption.

Finding the Balance in Encryption Legislation

Last year, certain US senators seemed determined to bring about the end of end-to-end encryption. Had they successfully passed the Lawful Access to Encrypted Data Act ("LAED Act") before the last Congress adjourned in December 2020, many device manufacturers and service providers would have been required to create methods to access and decrypt any data at rest or in motion, when presented with an applicable warrant. Additionally, upon request from the Attorney General of the United States, manufacturers and service providers would have been required to report within thirty days what they would do to access and decrypt the data and how long it would take to comply with the requirements.

In plain language, developers, manufacturers, and service providers would have been required to build vulnerabilities into products that provided end-to-end encryption. The crux of end-to-end encryption is that it is effective only because its goal is imperviousness to a man-in-the-middle attack – end-to-end encryption means that only the sender and the receiver see the unencrypted data. If a vulnerability is designed into the product, even for lawful purposes, the effectiveness, the level of protection, is necessarily reduced, and as such, it is only a matter of time before black hat hackers exploit that vulnerability. We know from even the most recent attacks, that black hat hackers are sophisticated and tenacious – if there is a way in – they will find it.

There are reasonable grounds to say that those who drafted the LAED Act were aware that any built-in backdoor to end-to-end encryption would be targeted by hackers, because this is not the first time that legislative attempts have been made to assist law enforcement with decrypting data. In 2015, a group of experienced, some well-known, computer scientists, published a technical report entitled, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* (https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf), in which they warned against exactly this issue by citing three general problems: (1) the erosion of best

practices in data protection; (2) an increase in complexity that would undermine security; and (3) the creation of "concentrated targets" upon which cyber-attacks would be focused (Ibid., Executive Summary). Ironically, many of the authors of this report were the same ones who authored a 1997 report in response to the *Clipper Chip* proposal, another early attempt to assist law enforcement decryption efforts.

Beyond criminal legal matters, would legislation of this type have an impact on civil litigants? As an example, we can look at *Gill v. Magan* (C19-860 MJP. *Dist. Court, WD Washington 2020*), wherein the Plaintiff was ordered by the Court to provide forensic examiners with her mobile phone and her passcode to facilitate the discovery of evidence. A reasonable hypothesis would allow that if manufacturers and service providers were required to create access and decryption functions as part of encryption products, would they not also be sought out eventually to perform that service as part of civil discovery? Why would a party not serve a subpoena or file for a Motion to Compel to invoke that function on a device when the device user simply refuses to cooperate in the discovery phase of litigation? At the very least, the threat of taking the device to the manufacturer or service provider would be a substantial one.

The serious questions raised by this proposed legislation are important ones and undoubtedly, this issue is not dead. To say the tech industry and governments need to work together on an acceptable balance between data privacy and crime prevention is an understatement. But there must be a balance, a fine line on which thoughtfully crafted legislation will balance the needs of law enforcement with the security of those law-abiding citizens who rely on technology such as end-to-end encryption to safeguard their personal and financial lives, as well as organizations protecting sensitive, valuable, and confidential data.

Please direct questions and inquiries about electronic discovery, computer forensics, cybersecurity and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

DATA CONNECTORS CYBERSECURITY CONFERENCE
Seattle & Portland: March 31, 2021 - April 1, 2021

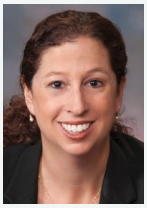
LEGALWEEK VIRTUAL SERIES 3
April 13, 2021

THE SEDONA CONFERENCE WORKING GROUP 11 ANNUAL MEETING 2021
April 14-15, 2021

IAPP GLOBAL PRIVACY SUMMIT 2021
April 27-28, 2021

THE SEDONA CONFERENCE WORKING GROUP 1 MIDYEAR MEETING 2021
April 28-29, 2021

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. In the short term, she is available for webinars and remote e-conferences.

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: