F20 Digital Evidence in Criminal Cases Before the United States Courts of Appeal: A Follow-Up Study on Trends and Issues for Consideration

Martin Novak, MPA, National Institute of Justice, Washington, DC 20531*

Learning Overview: After attending this presentation, attendees will: (1) understand the most relevant legal issues related to digital evidence, (2) understand precedent cases that impact digital evidence before the courts, (3) understand the most prevalent challenges to digital forensics, and (4) will discuss challenges on the horizon for digital evidence in criminal cases. Overall, attendees of this session will be informed as to how digital evidence has withstood challenges in appeals of criminal cases before the United States Courts of Appeal.

Impact on the Forensic Science Community: The current study is a follow-up to an American Academy of Forensic Sciences 2020 presentation.[1] The current study examines appeals of criminal cases before the United States Courts of Appeal from January 2016 through June 2020, where one or more appeal claims were related to digital evidence. The purpose of this research was to determine if the legal landscape has changed since 2015; examine the most relevant legal issues related to digital evidence; and analyze how precedent cases may have affected digital forensics as evidence.[2-5]

We live in a more connected world today than we did five years ago. Wearable devices have made their way into court as evidence recently, though their ultimate disposition as evidence is yet to be determined. Other important issues before the courts since 2015 include whether reasonable suspicion is necessary for an intrusive digital search at our nation's borders; whether compelling a suspect to provide their unlock code is "testimonial" for purposes of Fifth Amendment protection; the scope and particularity of digital search warrants when the government uses Network Investigative Techniques in online investigations, and finally whether the use of Cell Site Location Information (CSLI) for geo-location constitutes a search.

This analysis was based on a review of cases in the United States Circuit Courts of Appeals from 2016 through June 2020. Cases were identified via LexisNexis, using the following search terms: Probable Cause, Encryption, GPS, Geolocation, Geo-Fence, Onion Router, Wearables, Internet of Things, Text Message, Cryptocurrency, Network Investigative Tool (NIT), Particularity, Cell Phone, Metadata, Digital Evidence, Dark Web, ECPA, Social Media, and Child Pornography. Results include 80 criminal appeals before the United States Courts of Appeal. Of those cases, 88.75% were affirmed for the government. Offenses included possession and/or distribution of child pornography; narcotics possession or distribution; illegal weapons possession; armed robbery; sex crimes; violent offenses; and white collar crimes. The most frequently occurring basis for appeal was probable cause, followed by sufficiency of evidence, scientific merit, authenticity, and relevancy. In addition to the results, this presentation will discuss what has changed since 2015.

Reference(s):

1. Novak, Martin. Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law* 14, no. 4 (April 2020): 1-41. Accessed September 16, 2020. http://commons.erau.edu/jdfsl/vol14/iss4/3.
2. *Carpenter v. United States*, 138 S. Ct. 2206 (June 22, 2018.
3. *United States v. Levin*, 874 F.3d 316 (1st Cir. Oct. 27, 2017).
4. *United States v. Doe* (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. Feb. 23, 2012).
5. *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. May 9, 2018).

Digital Evidence, Compelled Decryption, Geo-Location

*Presenting Author