LITIGATION

January 2019 eDiscovery Update: Phones, Emails, Hash Values, and Saving Costs by Self-Authenticating ESI

By: Keith A. Langley

U.S. Supreme Court: Building a New Expectation of Digital Privacy?

In a criminal case that will prove applicable to civil cases, the U.S. Supreme Court dismissed a robbery count and carrying a firearm during a federal crime of violence as the government had access to cell site location information (CSLI). It ruled that seven days of access to CSLI was the product of a "search" and access to 127 days of historical CSLI invaded the defendant's reasonable expectation of privacy. Accordingly, the government had to obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier. The case was decided June 22, 2018. *Carpenter v. U.S.,* 138 S.CT. 2206 (2018).

The Court held through Justice Roberts that an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through CSLI; that seven days of CLSI was a search, and that Government's access to 127 days of historical CSLI invaded defendants reasonable expectation of privacy, and that Government must generally obtain a search warrant supported by probable cause before requiring CSLI from a wireless carrier. Justice Roberts relied upon a historical understanding of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. He stated that in light of the immense storage capacity of modern cell phones, police officers must generally obtain a warrant before searching the contents of a phone. Justice Roberts ruled that the police must obtain a search warrant before compelling the carrier to turn over a subscriber's CSLI. There was a discussion of exigent circumstances such as a fleeing suspect or protecting individuals who are threatened with imminent harm, or preventing the imminent destruction of evidence.

This topic dealt with the location of the defendant as shown by the cell phone. The information is detailed, and encyclopedic, and effortlessly compiled. We could see many changes in civil trials, especially the most expensive aspect of cases today: eDiscovery.

Beware of the limits on this ruling, and be on the lookout for its implications in civil cases.

LANGLEY | LLP
ATTORNEYS & COUNSELORS

Texas • Florida
Oklahoma • Arkansas

Dallas
1301 Solana Blvd.
Bldg. 1, Suite 1545
Westlake, Texas 76262
(214) 722-7160

Miami
1200 Brickell Avenue
Suite 1950
Miami, Florida 33131
(305) 961-1691

www.langley.law

***Adams v. Starside Custom Builders*, 547 S.W.3d 890 (Tex. 2018)**

This case from the Texas Supreme Court involved, as all cases now do, emails from the defendant alleging that the real estate developer felt it was defamed by the allegation in the email. The case was dismissed under the Texas Citizens Participation Act (TCPA). The Texas Supreme Court found that the email dealt with a matter of public concern under TCPA. Accordingly, the matter was dismissed and subject to a very fast dismissal. Further, an order denying a TCPA motion to dismiss is appealable. 547 S.W.3d at 892. Since the matter related to an issue of public concern, the Court of Appeals should have addressed the defamation case, the elements, and whether there was a valid defense under TCPA 27.005(b).

The Texas Supreme Court found that the email sent by the homeowner and wife were related to developers services in the marketplace, and there was a basis for dismissal under TCPA and further found that owners communications related to government or community well-being as further basis for dismissal under TCPA.

The complaint was dismissed because the TCPA allowed free speech of the homeowners and members of the homeowners association. Accordingly, accusations of failure to follow city ordinances regarding tree preservation as well as malfeasance and criminality of the developer concerned he well-being of the community as a whole.

New Federal Rules of Evidence Self-Authenticating ESI

Today, data copied from storage data and electronic files are ordinarily authenticated by "hash value". A hash value is a unique number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. *Litigation*, ABA, Fall 2018, New Evidence Rules and Artificial Intelligence, Hon. Paul W. Grimm, 9. Source Federal Rules of Evidence 902 (14) Advisory Committee Note (2017).

The chief problem associated with admissibility of digital information tends to be its authentication. Hash values provide an excellent mechanism for authenticating ESI. Last year, the U.S. Supreme Court further fixed this problem by promulgating Federal Rule of Evidence 902(13) and (14), providing for self-authentication of electronic evidence (e.g. ESI retrieved from a computer or copied to a USB), thereby helping streamline and reduce costs in the most expensive aspect of litigation: eDiscovery.

Keith Langley is a Partner at Langley LLP and may be contacted at klangley@l-llp.com.