SUMMER 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss relevant case law on smartphones, evidentiary value in cases and the increasing security threat from mobile malware.

Case Law Influencing Discoverability of Cell Phones

Despite the small, slim design of today's mobile phones, there remains a tangible inconvenience in carrying both a personal cell phone and a second device dedicated to work. Comingling all our portable electronic communication needs to one device eliminates the hassle of keeping both devices charged and ready. Additionally, if you're an entrepreneur watching expenses, or you work for a company that employs a "Bring Your Own Device" policy, footing the bill for one device instead of two may be just what the accountant ordered. However, is it wise, legally, to do so? Case law, as is often the case, is a beneficial source for helping make decisions on how to proceed when it comes to using a device for both work and personal communications, including generation, transmission, and storage of data.

The case law has and continues to come down fairly consistently with the idea that if you use a cell phone for both personal and work communications, including document production, storage, and/or transfer, that device is subject to a subpoena or search warrant, potentially exposing everything on the phone. In fact, one case considered to be a strong precedent on this topic is almost a decade old. In *State of New Mexico v. Marty Ortiz*, 146 N.M. 873, 215 P.3d 811 (2009), the court ruled that communications carried out on a personal cell phone during the hours an officer was on duty were relevant and subject to discovery by the defense.

In 2010, the US Supreme Court heard *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010), which concerned not cell phones, but pagers capable of receiving and sending text messages. When faced with charges for messaging that exceeded plan coverage, the police chief obtained full transcripts of officers' text messages to determine whether the officers had used their pagers for personal texting. The officers claimed this action violated their Fourth Amendment rights and rights to expectations of privacy. Upholding the legality of the search, and the extension of the

premise of “office space” to include the pagers, Justice Scalia wrote, “[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.” And while the Court felt it important to look at the case on “narrower ground,” it’s reasonable to say that the justices foresaw a larger issue looming on the technological horizon.

More recently, in *Nissen vs Pierce County*, 357 P.3d 45, 183 Wash.2d 863 (2015), the court went further and ordered, not just upheld after the event, “a transcript of the content of all the text messages at issue, review them, and produce to the County any that are public records,” thus exposing the personal communications stored on the phone to discovery, albeit not necessarily public disclosure.

To prevent discovery of personal communications, respondents have tried erasing stored information from phones, cancelling service and returning phones to vendors, and physically destroying devices. As effective as some of these methods may be for preventing the disclosure of personal information, the risk of adverse inference or sanctions for spoliation remains. The case of *National Football League Management Council, v. National Football League Players Association*, Nos. 15-2801 (L), 15-2805(CON) (2015), is one of the most high-profile cases with regard to phone destruction. New England Patriots quarterback Tom Brady was accused by the NFL of participating in an operation to contravene League rules by deflating footballs prior to a playoff game. The League suspended Brady for four games, relying in major part on the evidence that Brady had his personal cell phone destroyed, rendering it unsearchable. Brady’s refusal to cooperate with a directive to preserve electronic communications prior to the destruction, and Brady’s claim that he was unaware that the communications stored on his phone would be relevant to the investigation compounded the issue. On appeal, the court upheld the League’s adverse inference that Brady’s destruction of the phone could be interpreted as evidence that the phone contained information prejudicial to Brady’s defense. The Court’s analysis confirms the acceptance of cell phone data as evidence: “Finally, any reasonable litigant would understand that the destruction of evidence, revealed just days before the start of arbitration proceedings, would be an important issue.”

It’s not just employees who are looking to keep personal cell phones out of the court room. Employers seeking protection by establishing a BYOD policy to keep the devices at arm’s length from corporate liability should consider the case law when implementing policy. In *Hongsermeier v. USA Truck, et al*, No. 2:2016cv02321 - Document 38 (D. Kan. 2017), the court ruled that the personal cell phone records and data of an employee were material to the Plaintiff’s argument of a pattern of negligent employee behavior of which the company should have been aware. By using a personal cell phone while performing employment duties as a truck driver, the records and stored data became evidence of a pattern of distracted or dangerous driving, and outweighed the objections that the Defendant had already produced copious other materials in response to discovery.

Another consideration for BYOD policy use is the issue of “accidental syncing” between work and personal devices. Many mobile devices are set to automatically synchronize data when the mobile device is connected to a compatible device, such as a laptop or a desktop computer. While many people connect mobile devices to laptops or desktops simply to charge the cell phone, the automatic syncing function may unintentionally transfer data from one device to another, and therefore, unintentionally comingle personal and work data. While not covered by case law at this point, it’s reasonable to believe we’ll see a case that addresses the question of

discoverability of accidentally synced data in the future.

In light of the case law discussed above, we'd like to offer a few suggestions with regard to personal cell phone use for work and BYOD policies:

1. When possible, avoid using personal phones for work. Segregating personal communications from work communications using separate physical devices affords the most protection.
2. In the alternative, consider separate apps for similar communication types (email, messaging, etc.). In the event the phone must be searched, maintaining separate apps can make segregation of non-relevant information easier.
3. Consider mobile devices that offer dual user profiles and regularly confirm that data isn't "crossing the border."
4. For companies considering BYOD devices:
    a. Check employment laws, as well as wage and hour laws, for regulations which cover the use of personal cell phones for work. In addition to reimbursement for plan/data charges, some states require payment of wages for non-exempt employees who demonstrate via phone records that they conducted work duties outside their regular hours.
    b. Draft a policy which clearly reflects the company's expectations for the protection of company data stored on mobile devices.
    c. Include policy and procedure information on how company data on mobile devices will be collected following separation of employment.
    d. Communicate clearly that use of personal cell phones for work must be in compliance with applicable laws. As we discussed above, the policy may not entirely insulate a company from an employee's illegal use of a personal cell phone during employment hours; it may however demonstrate, along with application and enforcement of the policy, the company's diligent efforts.

We can reflect nostalgically about days gone by when the lines between work and personal life weren't blurred, but, that doesn't reverse the course of technology that provides us with the world instantaneously at our fingertips. What we can do is pay attention to what the case law tells us about comingling our work and personal lives on our cell phones, take steps to keep the data separate, and our personal information out of the courts. At Digital Mountain, beyond digital evidence preservation, collection and analysis of phones, we've been a redaction and escrow provider for cell phones and other devices for many years and have experienced continued growth in the need for segregating personal and business documents and communications.

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

UPCOMING INDUSTRY EVENTS

Black Hat USA
Las Vegas, NV: July 22-27, 2017

ILTACON 2017 Annual Educational Conference
Las Vegas, NV: August 13-17, 2017

PFIC 2017 Cyber Symposium
Pittsburgh, PA: August 18, 2017

Today's General Counsel, "The Exchange" eDiscovery
Houston, TX: September 13-14, 2017

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) 2017 Midyear Meeting
San Diego, CA: September 18-19, 2017

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: