Electronic Devices are **Witnesses**

A PARADIGM SHIFT FOR CLIENTS & LEGAL COUNSEL

WHITE PAPER

VESTIGE
Digital Investigations

Discovery

Conducting efficient and effective discovery that uncovers all the relevant evidence cost effectively.

- *Drafting a Request for Production of Documents.*
- *Understanding where data exists and how to ask for it.*
- *Drafting a Request For Production to ensure the production of active and inactive data including relevant artifacts.*
- *Examining of opposing Expert / IT Professional.*
- *Sample interrogatories and 30(b) Corporate depositions.*
- *Sample Motion Practice*

Electronic devices are everywhere. They come in all sizes and colors, and the trend seems to be that they get smaller and more powerful each year. They include computers, smart phones, medical devices, thumb drives, and a host of other devices, many of which remain invisible to us. A computer manages the operational functions of our vehicles, including, inter alia, monitoring RPM, throttle position, shift lever position, vacuum, oxygen, and the amount of weight placed on the passenger seat. Computers fly our airplanes, control temperature in our freezers, monitor our property when we are gone, and, of course, allow us to communicate across the Internet. In some situations, we may not even be aware that we are interacting with some form of electronic device. For example, a recent news report focused on employees in a hospital who were surprised to learn that their identification tags included a small Radio Frequency Identification Device (RFID) that was communicating with a computer to monitor employee hand washing and location on the hospital premises.[i]

> ***"In some situations, we may not even be aware that we are interacting with some form of electronic device."***

Searching for Documents in an Electronic World is a Trap. When faced with a duty to preserve electronic information, most attorneys become overwhelmed because they perceive that the duty to preserve requires that they identify each relevant electronic document no matter where it exists in the client's company. In many instances, attorneys believe that they must simply rely upon the client and/or key players to identify relevant information; hoping that the client can defend the protocols used by key players, hoping that data is not changed during the preservation process, and hoping that the client will understand the scope of discoverable information. Even if an attorney wants to identify sources of discoverable information, there is a perception that this process is very difficult because counsel does not know anything about the client's electronic information systems. Moreover, when counsel attempts to learn about the client's information systems, counsel is frequently confused by the terms and concepts used by IT professionals. Finally, counsel

may be overwhelmed by the prospect of identifying the electronic evidence that resides upon electronic devices due to the sheer volume of data. Counsel may think that finding electronic evidence in the client's information systems requires counsel and key players wander about the information system hoping to locate relevant data. These perceptions lead counsel to believe that electronic discovery is necessarily time consuming, disruptive, and costly. These perceptions also lead counsel to believe that there are no choices in electronic discovery and that strategic use of electronic evidence is not possible except in very large cases or to obtain settlement to avoid discovery.[ii]

Devices as Witnesses

This is a fundamental shift in thinking that will naturally prevent attorneys from getting lost trying to find individual, relevant, documents amidst a sea of millions of documents stored on electronic devices.

Quit Looking for Documents—Treat the Devices on which the Documents reside as "Witnesses". Many of these misperceptions about electronic discovery can be corrected by treating the electronic devices used by key players as if each device was, itself, a witness in the case. Treating electronic devices as witnesses is possible because the devices have two characteristics that make them act like a human witness: they contain electronic memory and they process/create information on their own.

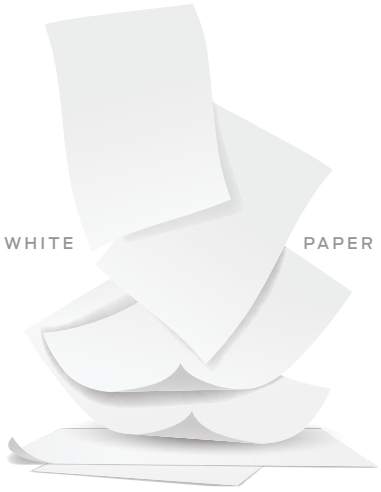
An electronic device's memory allows it to store information, like a human witness who remembers the documents the witness created that are relevant to the matter. In this regard, electronic devices are "fact" witnesses, capable of being searched to produce the relevant electronic documents created by key players.

The processing capability of each electronic device allows each device to also be an "event witness" – recording the manner in which they were used. As described in greater detail in future installments of the Vestige Guide, electronic devices automatically store information about the manner in which they are being used at any time. This information is created—not by the key player using the device—but rather by the file system, operating system and applications installed on the device. Event information created by the device can be analyzed and the manner in which the device was used can be "recreated". In this fashion, electronic devices are "event" witnesses.

Rule: Electronic Devices are Witnesses. Treating the devices as witnesses naturally causes attorneys to identify those devices used by key players as potential sources of discoverable information—not because the attorney has identified any particular documents resident on the device; but rather because the key player used the device. This is a fundamental shift in thinking that will naturally prevent attorneys from getting lost trying to find individual, relevant, documents amidst a sea of millions of documents stored on electronic devices. We will discuss in later updates the manner in which the entire device can be quickly preserved (without spending any time or effort to search the device for specific documents). At the initial stages of using electronic evidence, however it is fortunate that counsel can identify the devices as electronic witnesses because they have been used by key players because this skill does not require any technical training.

[i] "FL Hospital Uses RFID to Monitor Employee Hand Washing", RFID News, August 3, 2009 available at www.rfidnews.org/2009/08/03/fl-hospital-uses-rfid-to-monitor-employee-hand-washing.

[ii] See InformationWeek, December 8, 2008 "E-Discovery's Terrible Twos".



.VESTIGE
Digital Investigations

For more information Contact us today
800.314.4357 or info@vestigeltd.com