Divorce Data and Spying:

Ethical and Legal Implications

Faculty:

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

Lisa McNorton
McNorton Fox PLLC
Lisa@McNortonFoxLaw.com
www.McNortonFoxLaw.com

esi evidence solutions, inc.

MF McNORTON FOX PLLC

Famous Quote

- Bill Gates once said: "If GM had kept up with the technology like the computer industry has, we would all be driving $25.00 cars that got 1,000 miles to the gallon."

- If GM had developed technology like Microsoft, cars would:
  - When your car died on the freeway for no reason, you would just accept this, restart and drive on.
  - Apple would make a car powered by the sun, reliable, five times as fast, and twice as easy to drive, but would run on only five per cent of the roads.
  - The airbag would say 'Are you sure?' before going off.
  - Every time GM introduced a new model, car buyers would have to learn how to drive all over again because none of the controls would operate in the same manner as the old car.
  - You would press the 'start' button to shut off the engine.

Some Definitions

- Electronic Discovery / E-Discovery / eDiscovery
- The process in which electronic evidence is:
  - Sought
  - Identified
  - Collected / preserved
  - Processed /Reviewed
  - Analyzed
  - Produced
  - Presented
- Usually on a Hosted eDiscovery Platform

Some Definitions

- Digital Forensics
  - Computers
  - Cell phones
  - Cars / trucks
  - Electronic Medical Records
  - Hacking
  - Etc.

GENERAL COMPUTER FORENICS

Evidence Collection
Sources of Evidence:

- Storage Media includes:
  - Hard Disk Drives
  - Backup tapes
  - DVD / CD Rom disks
  - E-prom and Memory chips
  - Thumb Drives
  - iPods, iPads & MP3 Players
  - Cell Phones
  - The Cloud
  - Infotainment Systems

Evidence Collection

- Storage Media
  - Because data is easily destroyed, when the data arrives at the lab, the first priority of the investigator is to preserve integrity of the evidence.
  - Just turning on the machine and allowing the system to boot, will cause irreparable changes to the data…..

Metadata

- **Metadata:** Metadata is “data about data.” Metadata can be attached or associated with various types of ESI including: Document Files, Photos, SMS Messages, Messages, as well as physical items such as CDs and DVDs.

Metadata

- Photographs
- Electronic Medical Records
- Vehicles
- Email
- Documents / Spreadsheets
- File System Metadata

Evidence Collection

- **Hard Drive Image**
  or
  Mirror Image
  or
  Forensic Image:

- This is a bit-by-bit copy of storage media. (i.e., an exact copy of a physical Hard Drive).

Evidence Collection

- **Hash or Digital Fingerprint:**
  - A hash value is a unique hexadecimal value identifying lines of text, a file or Hard Drive Image. The value serves as an identifying fingerprint, and is even more unique human DNA. The value is generated via mathematical algorithm; the de facto algorithm still used is Message Digest-5, or MD5 for short. Others include SHA-1, SHA-256, etc.

Evidence Collection / Hashes

- “The quick brown fox jumps over the lazy dog”
  - 9e107d9d372bb6826bd81d3542a419d6
- “The quick brown fox jumps over the lazy cog”
  - ffd93f16876049265fbaef4da268dd0e

File Dates

- **Date Created:**
  - The date and time that this file was created on this machine, this would include the date downloaded from the Internet.
- **Date Modified:**
  - The date and the time the file was last modified. This may also include downloading from the Internet. This date normally follows the file around and doesn't change unless the file changes.
- **Date Accessed:**
  - This is the last date that the file was accessed for reading by the machine or user.

How not to do things….

- The law firm overwrote the data!!!!
  - The machine was on when we arrived.
  - The owner of the machine had rigged the machine with some pretty sophisticated software that automatically overwrote key data files when the machine was booted and a question was either skipped or answered wrong in the boot process.
  - The data that the law firm sought was completely destroyed.

How not to do things….

- The IT department overwrote the data!!!
  - Employee deleted data from hard disk drive
    - but didn't delete it from the recycle bin
  - Technology department recovered the data using some standard data tools
    - but destroyed the evidence that proved the employee deleted the data in the first place
    - this made our job much much harder than it had to be

INFOTAINMENT SYSTEMS

Infotainment Systems

Infotainment Systems

- BMW
- Buick
- Cadillac
- Chevrolet
- Chrysler
- Dodge
- FIAT
- Ford
- GMC
- HUMMER
- Jeep
- Lincoln
- Maserati
- Mercury
- Pontiac
- Ram
- Saturn
- SEAT
- Skoda
- SRT
- Toyota
- Volkswagen

Infotainment Systems

- **Vehicle/System Information**
  - Serial Number
  - Part Number
  - Original VIN Number
  - Build Number
- **Installed Application Data**
  - Weather
  - Traffic
  - Facebook
  - Twitter
- **Connected Devices**
  - Phones
  - Media Players
  - USB Drives
  - SD Cards
  - Wireless Access Points
- **Navigation Data**
  - Tracklogs and Trackpoints
  - Saved Locations
  - Previous Destinations
  - Active and Inactive Routes
- **Device Information**
  - Device IDs
  - Calls
  - Contacts
  - SMS
  - Audio
  - Video
  - Images
  - Access Point Information

Infotainment Systems

- **Events**
  - Doors Opening/Closing
  - Lights On/Off
  - Bluetooth Connections
  - Wi-Fi Connections
  - USB Connections
  - System Reboots
  - GPS Time Syncs
  - Odometer Readings
  - Gear Indications

Infotainment Systems

- Loaning your car to someone would allow them, with the help of a professional, to collect the data from the Infotainment System.

CELL PHONES

Digital Evidence: Cell Phone Forensics

- **Cell Phones & Tablets**
  - Text messages
  - Photos?
    - GeoTagging
  - Calendars
  - Phone Books
  - Call Logs
  - Complete information about where the phone has been….

Digital Evidence: Cell Phone Forensics

- **Cell Phones & Tablets**
  - Browsing History
  - Documents
  - Email Accounts
  - Online Data Storage Accounts

Digital Evidence: Cell Phone Forensics

- **Cell Phones & Tablets Spying Software**
  - Mspy
  - Mobi Stealth
  - Spy Bubble
  - Spy Phone Tap
  - And others

Digital Evidence: Cell Phone Forensics

- **Spying Software Capabilities**
  - Monitor / Record Calls
  - Record Surroundings
  - SMS & MMS
  - GPS Location
  - Internet Use
  - Remote Access to:
    - Calendar
    - Contacts
  - SMS / Instant Messages
  - Photos & Videos
  - Turn on Camera & Microphone
  - Remote Control

- One site that sells some Spy Equipment:
  - "… all you have to do is obtain permission from the phone's owner/user, install a small application on the phone …"
  - Then you can monitor their whereabouts, track them by GPS, read their email, and read their text messages.
  - Warning: The description stops short of warning the purchaser to check local laws or consult an attorney prior to purchase or use.

Warning!!!

WEB BROWSING ARTIFACTS

Artifacts From Web Browsing

- The value of seeing what a person is searching for in the Internet can be key.

Artifacts From Web Browsing

- http://wiki.answers.com/Q/How_can_you_help_a_sociopath?#slide=59

- How can you help a sociopath? - Answers.com

Artifacts From Web Browsing

- http://www.subito.it/appartamenti/appartamento-a-grutti-di-gualdo-cattaneo-rif-301-perugia-77278016.htm

- Appartamento in castello di Grutti - Appartamenti In vendita a Perugia

Artifacts From Web Browsing

- http://mysecurewallet.nl/payment/islive/isliveeu/?p=199&pi=typein_isliveeu&flash=1&m=bellaluna

- My Secure Wallet

Spying Devices

- Other Sources of Evidence

GPS Tracking Devices

GPS Tracking Devices

Spying Equipment

Spying Equipment

Spying Equipment

- Keyloggers
- Spying Software
  - Computers
  - Cell Phones
- Hidden Cameras

"Digital Evidence is Everywhere!"

- Email Systems
  - Data is Easily Fabricated
- Telematics / Electronic Logging Devices
  - They aren't the end
- Self Driving / Automation in Cars
  - Safer…. eventually

"Digital Evidence is Everywhere!"

Faculty:

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

Lisa McNorton
McNorton Fox PLLC
Lisa@McNortonFoxLaw.com
www.McNortonFoxLaw.com

For additional resources please visit:
www.EvidenceSolutions.com/AAML