Evidence Solutions, Inc.

And the

Southern Arizona Estate Planning Council

Present:

Digital Security in a Business Setting

September 13, 2017

Arizona Inn
2200 E Elm St
Tucson, AZ 85719

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc.

Digital Forensics Firm

520-512-5001
866-795-7166

Scott@EvidenceSolutions.com

esi
evidence solutions, inc.

Biography

Scott Greene

Scott is the CEO of Evidence Solutions, Inc. Scott Greene has been doing Data Recovery, Computer, Technology and Digital Forensics, and EDiscovery work for over 35 years.

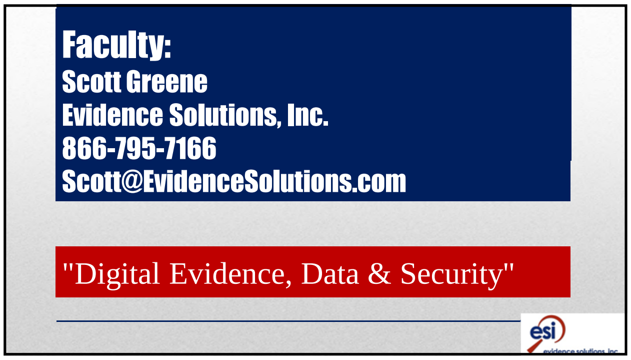
Directly out of high school, Scott went to work for IBM as a programmer.

In 2008 he created Evidence Solutions, Inc., a full service Computer, Technology & Digital Forensics firm, from the Technology Forensics department of Great Scott Enterprises.

Scott has developed and presented strategic planning seminars, taught numerous classes in database design & optimization, cyber security and technology forensics. Scott's extensive knowledge draws clients to him from all over the United States as well as Internationally for consulting and expert witness services in the field of Technology, Computer & Digital Forensics. His extensive and diverse experience allows him to be an expert in many facets of computer & digital technology.

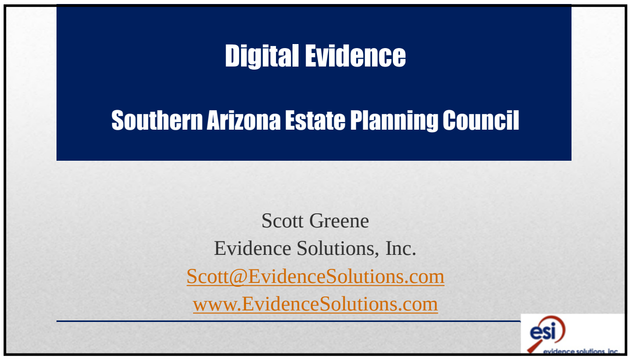
Scott and Evidence Solutions have been involved in Civil & Criminal Cases, for Plaintiff, Defense and Special Master in Justice, Superior & District Courts as well as Internationally.

He is a sought after speaker and educator and travels throughout the country presenting to local, regional, national and International organizations.



Faculty:
Scott Greene
Evidence Solutions, Inc.
866-795-7166
Scott@EvidenceSolutions.com

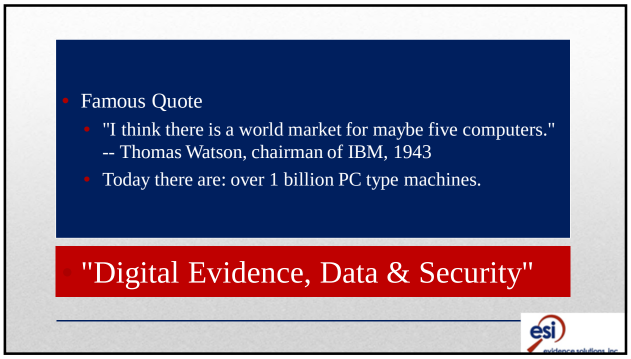
"Digital Evidence, Data & Security"



Digital Evidence

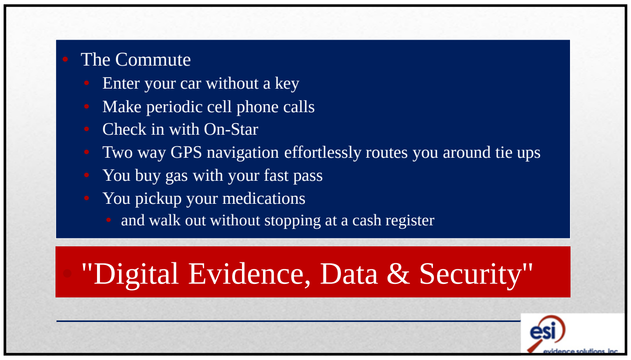
Southern Arizona Estate Planning Council

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



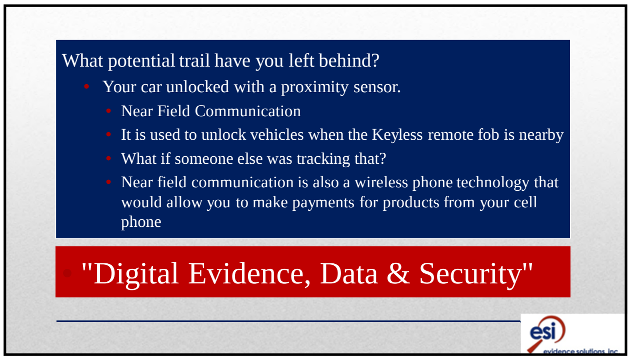
- Famous Quote
  - "I think there is a world market for maybe five computers." -- Thomas Watson, chairman of IBM, 1943
  - Today there are: over 1 billion PC type machines.

"Digital Evidence, Data & Security"



- The Commute
  - Enter your car without a key
  - Make periodic cell phone calls
  - Check in with On-Star
  - Two way GPS navigation effortlessly routes you around tie ups
  - You buy gas with your fast pass
  - You pickup your medications
    - and walk out without stopping at a cash register

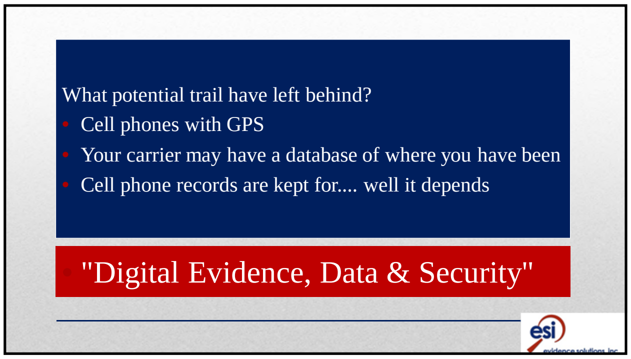
"Digital Evidence, Data & Security"



What potential trail have you left behind?

- Your car unlocked with a proximity sensor.
  - Near Field Communication
  - It is used to unlock vehicles when the Keyless remote fob is nearby
  - What if someone else was tracking that?
  - Near field communication is also a wireless phone technology that would allow you to make payments for products from your cell phone

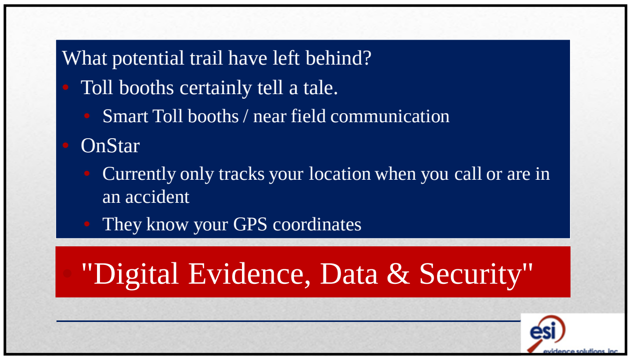
"Digital Evidence, Data & Security"



What potential trail have left behind?

- Cell phones with GPS
- Your carrier may have a database of where you have been
- Cell phone records are kept for.... well it depends

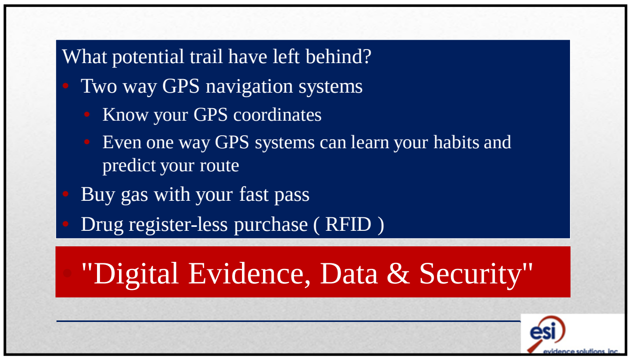
"Digital Evidence, Data & Security"



What potential trail have left behind?

- Toll booths certainly tell a tale.
  - Smart Toll booths / near field communication
- OnStar
  - Currently only tracks your location when you call or are in an accident
  - They know your GPS coordinates

"Digital Evidence, Data & Security"



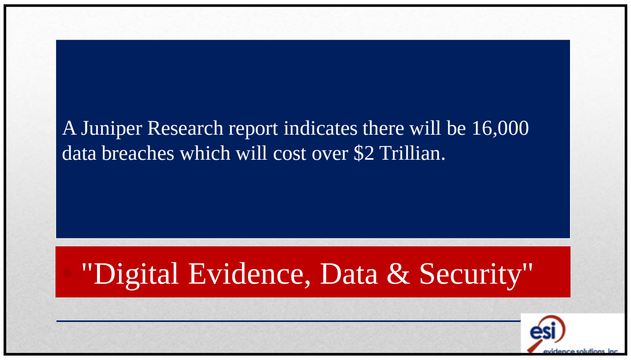
What potential trail have left behind?

- Two way GPS navigation systems
  - Know your GPS coordinates
  - Even one way GPS systems can learn your habits and predict your route
- Buy gas with your fast pass
- Drug register-less purchase (RFID)

"Digital Evidence, Data & Security"

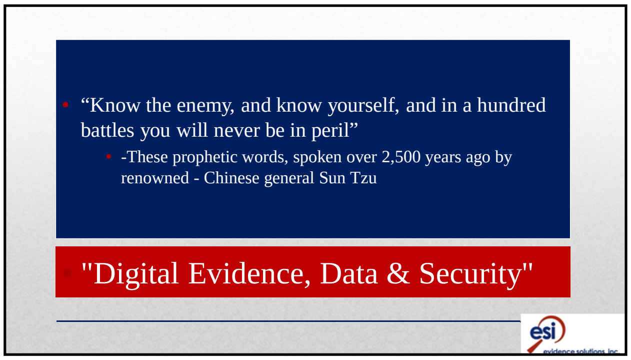
Security!

"Digital Evidence, Data & Security"



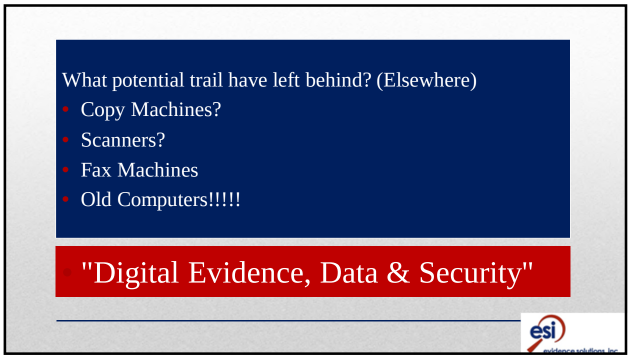
A Juniper Research report indicates there will be 16,000 data breaches which will cost over $2 Trillian.

"Digital Evidence, Data & Security"



- “Know the enemy, and know yourself, and in a hundred battles you will never be in peril”
  - -These prophetic words, spoken over 2,500 years ago by renowned - Chinese general Sun Tzu

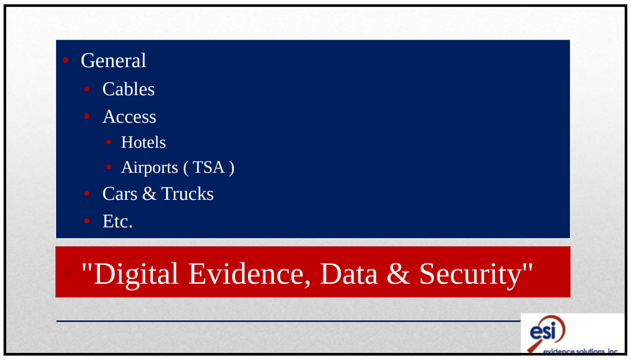
"Digital Evidence, Data & Security"



What potential trail have left behind? (Elsewhere)

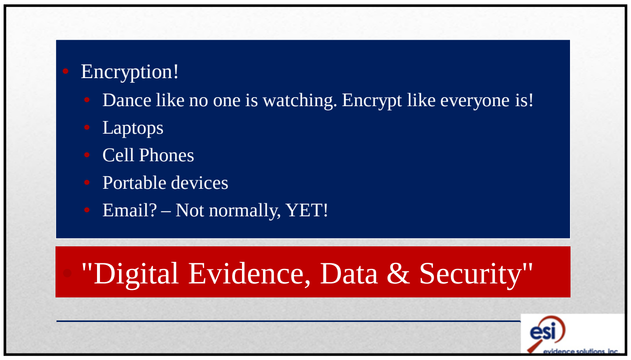
- Copy Machines?
- Scanners?
- Fax Machines
- Old Computers!!!!!

"Digital Evidence, Data & Security"



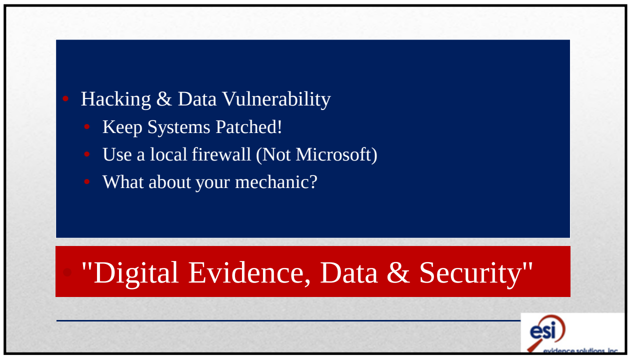
- General
  - Cables
  - Access
    - Hotels
    - Airports (TSA)
  - Cars & Trucks
  - Etc.

"Digital Evidence, Data & Security"



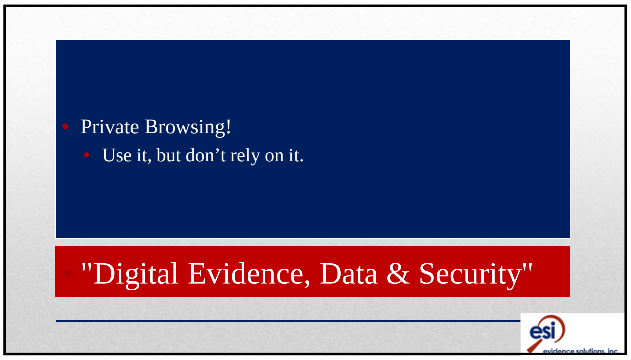
- Encryption!
  - Dance like no one is watching. Encrypt like everyone is!
  - Laptops
  - Cell Phones
  - Portable devices
  - Email? – Not normally, YET!

"Digital Evidence, Data & Security"



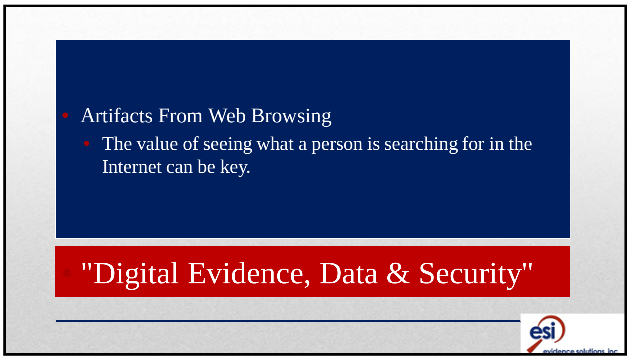
- Hacking & Data Vulnerability
  - Keep Systems Patched!
  - Use a local firewall (Not Microsoft)
  - What about your mechanic?

"Digital Evidence, Data & Security"



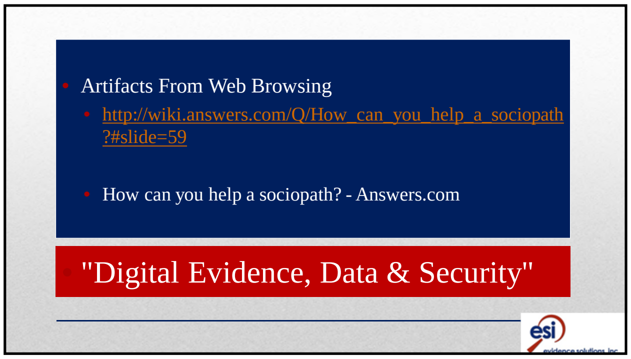
- Private Browsing!
  - Use it, but don’t rely on it.

"Digital Evidence, Data & Security"



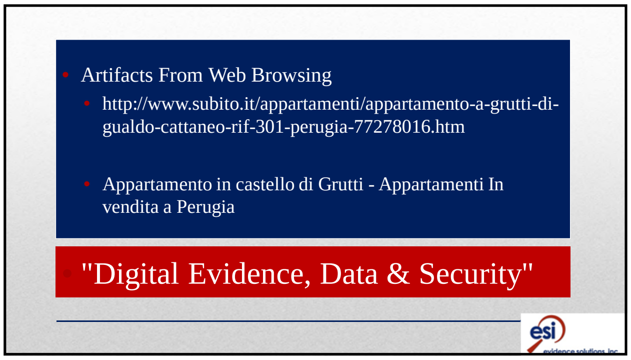
- Artifacts From Web Browsing
  - The value of seeing what a person is searching for in the Internet can be key.

"Digital Evidence, Data & Security"



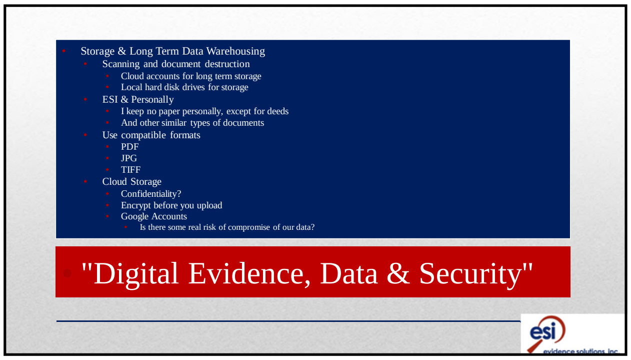
- Artifacts From Web Browsing
  - http://wiki.answers.com/Q/How_can_you_help_a_sociopath?#slide=59
  - How can you help a sociopath? - Answers.com

"Digital Evidence, Data & Security"



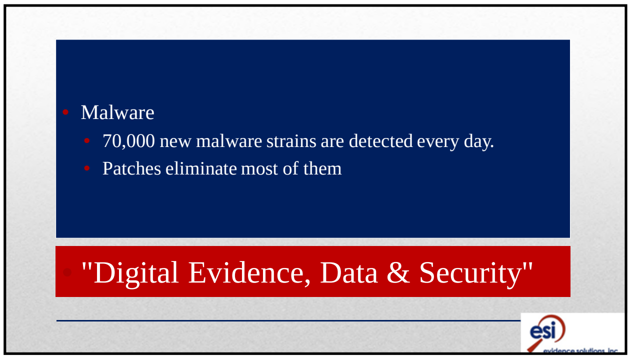
- Artifacts From Web Browsing
  - http://www.subito.it/appartamenti/appartamento-a-grutti-di-gualdo-cattaneo-rif-301-perugia-77278016.htm
  - Appartamento in castello di Grutti - Appartamenti In vendita a Perugia

"Digital Evidence, Data & Security"



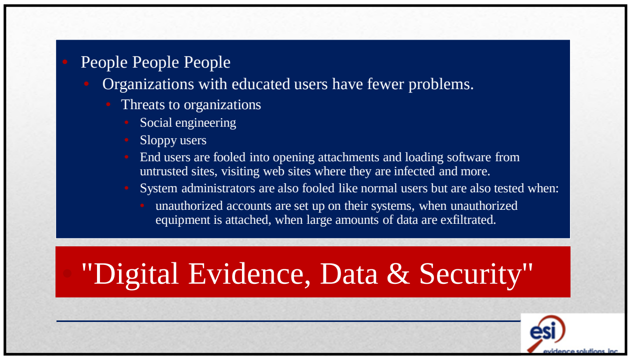
- Storage & Long Term Data Warehousing
  - Scanning and document destruction
    - Cloud accounts for long term storage
    - Local hard disk drives for storage
  - ESI & Personally
    - I keep no paper personally, except for deeds
    - And other similar types of documents
  - Use compatible formats
    - PDF
    - JPG
    - TIFF
  - Cloud Storage
    - Confidentiality?
    - Encrypt before you upload
    - Google Accounts
      - Is there some real risk of compromise of our data?

"Digital Evidence, Data & Security"



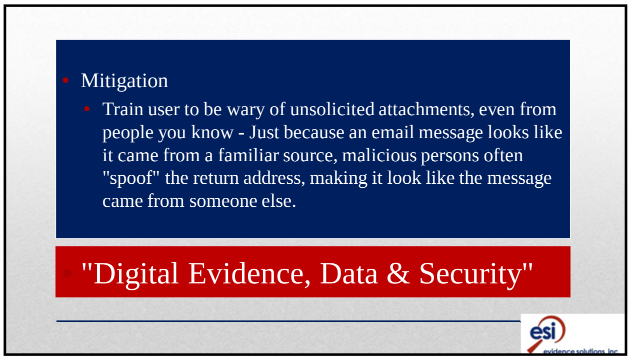
- Malware
  - 70,000 new malware strains are detected every day.
  - Patches eliminate most of them

"Digital Evidence, Data & Security"



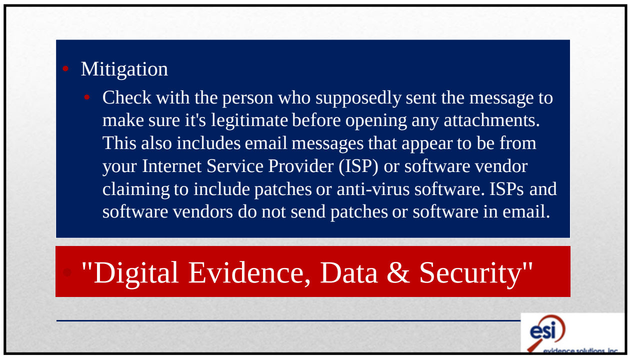
- People People People
  - Organizations with educated users have fewer problems.
    - Threats to organizations
      - Social engineering
      - Sloppy users
      - End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected and more.
      - System administrators are also fooled like normal users but are also tested when:
        - unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data are exfiltrated.

"Digital Evidence, Data & Security"



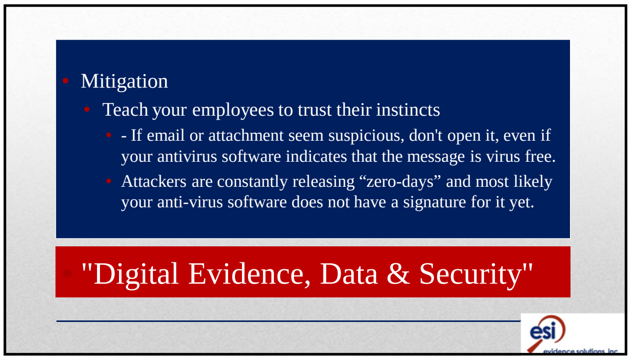
- Mitigation
  - Train user to be wary of unsolicited attachments, even from people you know - Just because an email message looks like it came from a familiar source, malicious persons often "spoof" the return address, making it look like the message came from someone else.

"Digital Evidence, Data & Security"



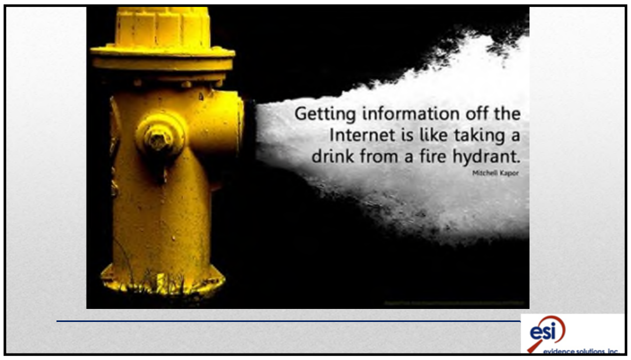
- Mitigation
  - Check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This also includes email messages that appear to be from your Internet Service Provider (ISP) or software vendor claiming to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

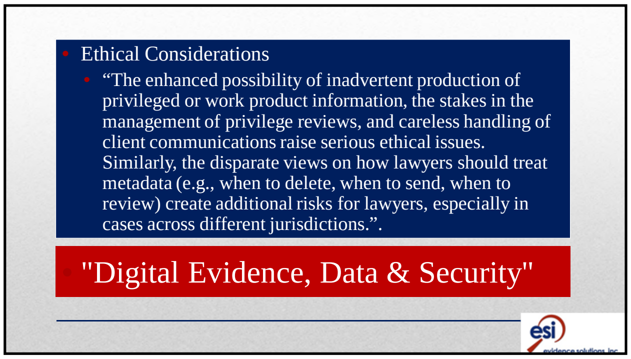
"Digital Evidence, Data & Security"



- Mitigation
  - Teach your employees to trust their instincts
    - - If email or attachment seem suspicious, don't open it, even if your antivirus software indicates that the message is virus free.
    - Attackers are constantly releasing “zero-days” and most likely your anti-virus software does not have a signature for it yet.

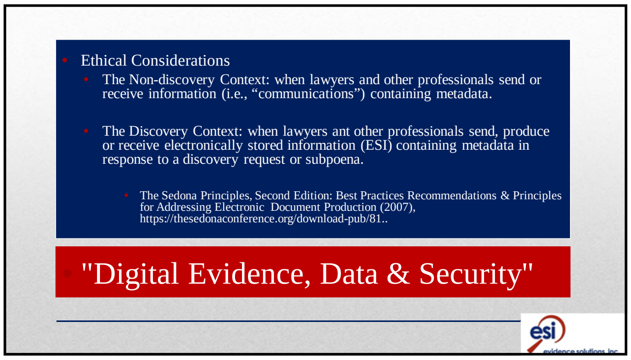
"Digital Evidence, Data & Security"


Getting information off the Internet is like taking a drink from a fire hydrant.
Mitchell Kapor



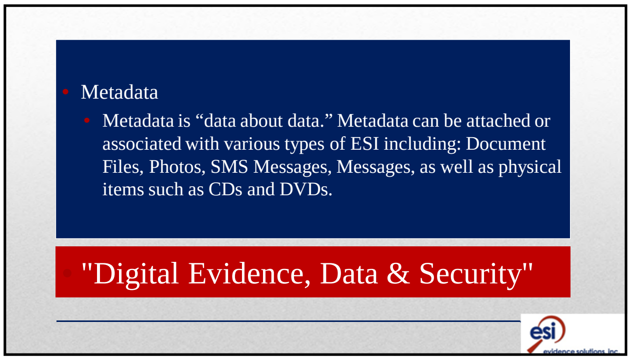
- Ethical Considerations
  - “The enhanced possibility of inadvertent production of privileged or work product information, the stakes in the management of privilege reviews, and careless handling of client communications raise serious ethical issues. Similarly, the disparate views on how lawyers should treat metadata (e.g., when to delete, when to send, when to review) create additional risks for lawyers, especially in cases across different jurisdictions.”.

"Digital Evidence, Data & Security"



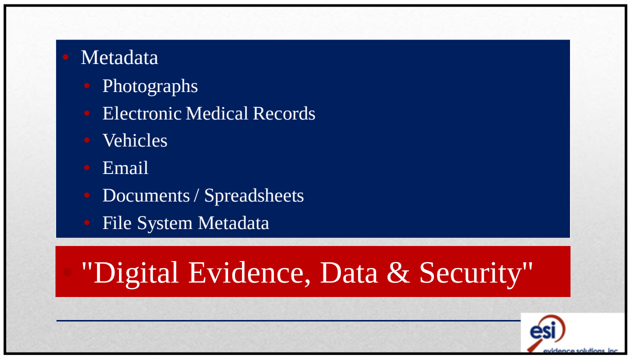
- Ethical Considerations
  - The Non-discovery Context: when lawyers and other professionals send or receive information (i.e., “communications”) containing metadata.
  - The Discovery Context: when lawyers ant other professionals send, produce or receive electronically stored information (ESI) containing metadata in response to a discovery request or subpoena.
    - The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production (2007), https://thesedonaconference.org/download-pub/81..

"Digital Evidence, Data & Security"



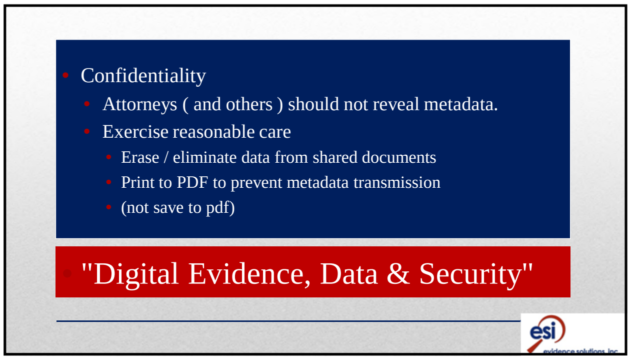
- Metadata
  - Metadata is “data about data.” Metadata can be attached or associated with various types of ESI including: Document Files, Photos, SMS Messages, Messages, as well as physical items such as CDs and DVDs.

"Digital Evidence, Data & Security"



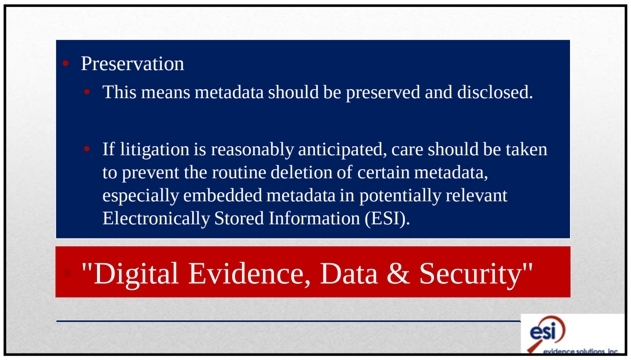
- Metadata
  - Photographs
  - Electronic Medical Records
  - Vehicles
  - Email
  - Documents / Spreadsheets
  - File System Metadata

"Digital Evidence, Data & Security"



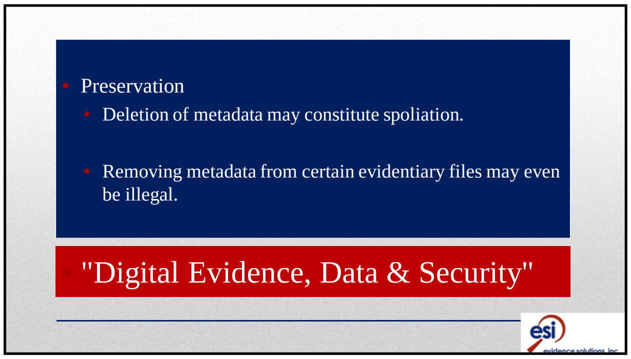
- Confidentiality
  - Attorneys (and others) should not reveal metadata.
  - Exercise reasonable care
    - Erase / eliminate data from shared documents
    - Print to PDF to prevent metadata transmission
    - (not save to pdf)

"Digital Evidence, Data & Security"



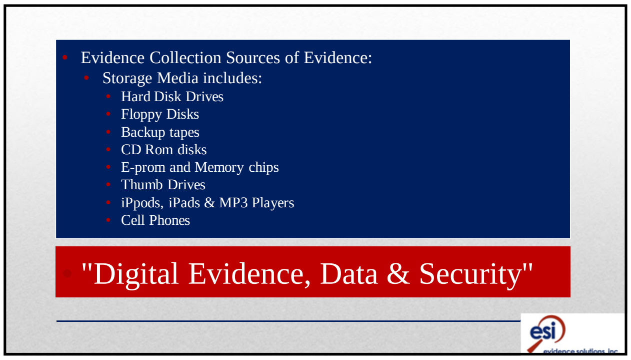
- Preservation
  - This means metadata should be preserved and disclosed.
  - If litigation is reasonably anticipated, care should be taken to prevent the routine deletion of certain metadata, especially embedded metadata in potentially relevant Electronically Stored Information (ESI).

"Digital Evidence, Data & Security"



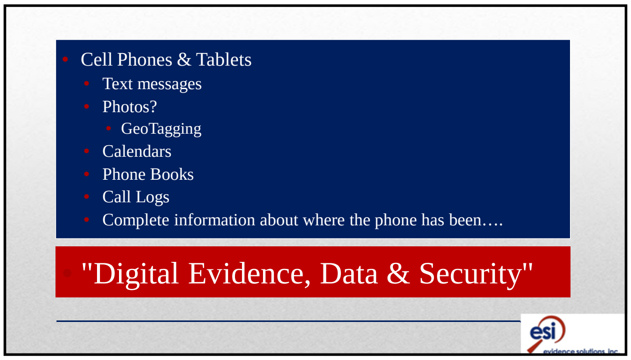
- Preservation
  - Deletion of metadata may constitute spoliation.
  - Removing metadata from certain evidentiary files may even be illegal.

"Digital Evidence, Data & Security"



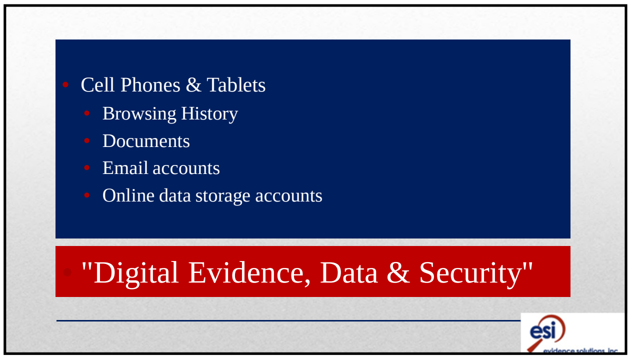
- Evidence Collection Sources of Evidence:
  - Storage Media includes:
    - Hard Disk Drives
    - Floppy Disks
    - Backup tapes
    - CD Rom disks
    - E-prom and Memory chips
    - Thumb Drives
    - iPpods, iPads & MP3 Players
    - Cell Phones

"Digital Evidence, Data & Security"



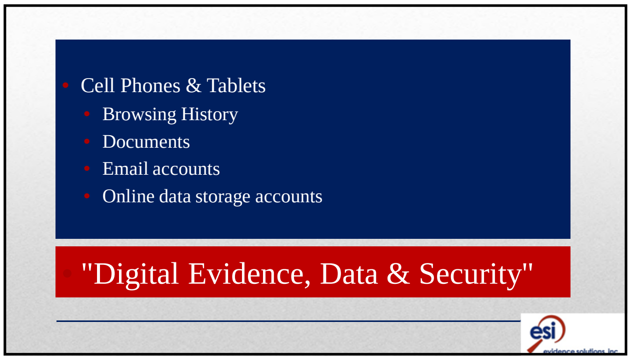
- Cell Phones & Tablets
  - Text messages
  - Photos?
    - GeoTagging
  - Calendars
  - Phone Books
  - Call Logs
  - Complete information about where the phone has been….

"Digital Evidence, Data & Security"



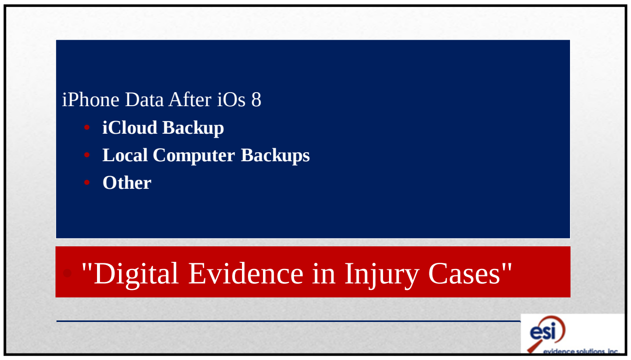
- Cell Phones & Tablets
  - Browsing History
  - Documents
  - Email accounts
  - Online data storage accounts

"Digital Evidence, Data & Security"



- Cell Phones & Tablets
  - Browsing History
  - Documents
  - Email accounts
  - Online data storage accounts

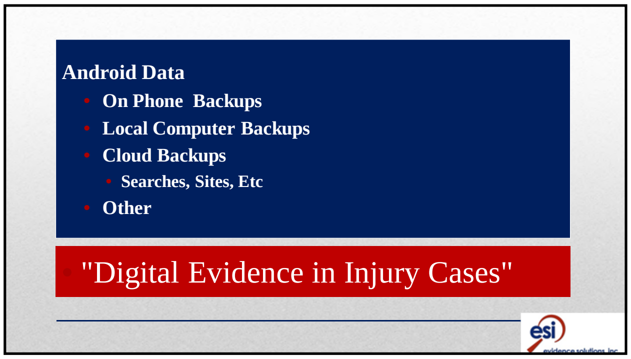
"Digital Evidence, Data & Security"



iPhone Data After iOs 8

- **iCloud Backup**
- **Local Computer Backups**
- **Other**

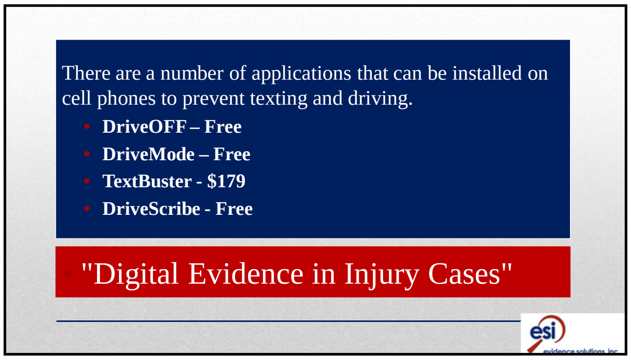
"Digital Evidence in Injury Cases"



Android Data

- **On Phone Backups**
- **Local Computer Backups**
- **Cloud Backups**
  - **Searches, Sites, Etc**
- **Other**

"Digital Evidence in Injury Cases"



There are a number of applications that can be installed on cell phones to prevent texting and driving.

- **DriveOFF – Free**
- **DriveMode – Free**
- **TextBuster - $179**
- **DriveScribe - Free**

"Digital Evidence in Injury Cases"

Scott Greene, President &
Senior Technology Examiner

esi
evidence solutions, inc.

866.795.7166 (toll free)
520.722.6796 (fax)

www.evidencesolutions.com
info@evidencesolutions.com

Scott@EvidenceSolutions.com

evidence solutions, inc.

Seminar Evaluation Form

Date: _____ ____________________

	Poor	Ok	Good	Very Good	Excellent
1. Was the material informative?	**1**	**2**	**3**	**4**	**5**
2. Was the material easy to understand?	**1**	**2**	**3**	**4**	**5**
3. Was the material appropriate?	**1**	**2**	**3**	**4**	**5**
4. Was the material interesting?	**1**	**2**	**3**	**4**	**5**
5. Was the medium used to present this subject effective?	**1**	**2**	**3**	**4**	**5**
6. The material presented in the seminar will be of use to me.	**1**	**2**	**3**	**4**	**5**
7. The material presented was properly sequenced.	**1**	**2**	**3**	**4**	**5**
8. Was the speaker effective?	**1**	**2**	**3**	**4**	**5**
9. The seminar was well worth my time.	**1**	**2**	**3**	**4**	**5**

10. Have you relied on computer forensics in your previous experience? **YES** _____ **NO** _____

12. General impression of material presented? ____

____

____

13. Why did you attend this seminar today? ____

____

____

14. Would you like someone to contact you about computer forensics? **YES** ______ **NO** ______

Name: ____

Address: ____

Mailing Address: ____
(if different)

Email: ____

Phone: (   ) ____________________ **Fax:** (   ) ____________________

Comments may be used on EvidenceSolutions.com. Please let me know if you object.