How to “Like” E-Discovery, Security and Social Media

Dr. Gavin W. Manes, CEO
Gavin W. Manes, Ph.D.

• CEO, Avansic
• Doctorate in Computer Science from TU
• Scientific approach to e-discovery
• Published over fifty papers on e-discovery, forensics and security, presented at hundreds of events
• Expert witness
ESI Processing

**IDENTIFICATION & STRATEGY**
Data, Custodians, IT, Standards

**PRESERVATION**
- Devices
  - Computer, Server Shares, Sharepoint, Tape, Other
- Web Data
  - Email, Mobile, Cloud Storage, Third Party

**COLLECTION**
- Select Data, Remote/Self Collection
- Forensics Copy

**PROCESSING**
- Filter/Cull
  - Date, search term, file type, de-NIST
- De-Dupe
  - Cross-Custodian
- Imaging
  - TIFF, PDF, OCR, Searchable
- Metadata
  - Common, Detail
- Clustering
  - Related Documents, Ordering, near-dupe

**REVIEW & ANALYSIS**
- Document Review
  - Online, Native, TIFF images
- Technology Assisted Review
- Forensics Investigation

**PRODUCTION**
- Loadfiles, Reports, Native, Files, Online
  - Secure Transfers
    - Dii, Dat/Opt, DCB, and others
- Recovery
  - deleted, broken, double-deleted

E-Discovery, Security and Social Media

AVANSIC ESI PROCESSING
copyright 2013 Avansic, Inc.
for more detail visit
http://www.avansic.com/EsiProcessing
Who are the Players?

• **Clients/Corporations**
  – Organize and know where data is
  – Continue doing business – carefully

• **Law Firm**
  – Direct discovery
  – Plan and strategize EARLY
  – Choose technology partners [vendor, in-house, client]
  – Review and redact

• **ESI vendor**
  – Communicate well with parties
  – Recommend best course of action based on experience
  – Manage expectations
  – Execute project plan as efficiently as possible
What Are the Legal Team’s Choices?

• **Preservation**
  – Use client resources; hire vendor; use law firm’s staff

• **Processing**
  – Hire vendor; use client or law firm resources; some of each
  – Search terms; deduplication; email threading;

• **Review**
  – Use analytics and concept clustering; use predictive coding or technology assisted review; put eyes on every document
  – Use hosted review tool; use PDFs, fileshares and spreadsheets; use desktop review tool; internally host tool at the firm
  – Use contract reviewers; use law firm reviewers; use client reviewers

• **Production**
  – Use review tool to package documents into loadfiles; use PDFs
Small Sized E-Discovery Case Examples

• Opposing counsel sends over a DVD with the results of a keyword search: a PST of someone’s email and a hundred loose files
• Need to find all the text messages to and from a specific phone number on one person’s cell phone
• Client gives you a hard drive with four PSTs in order to determine correspondence with keywords within a two week timeframe
• Scan one box of paper documents, including 4 CDs, to online review tool for attorney review
Small Sized E-Discovery Case Choices

• Collection options: corporate IT create a copy of the email store and hard drive (careful!), forensic copy created by vendor
• Processing options: no processing, load to simple online processing/review tool, vendor indexing, filtering, de-dupe
• Review options: straight review of the images by attorney, load to review tool (desktop or hosted)
• Production options: create pdfs, produce from desktop/hosted tool
• Or, a hybrid
Medium Sized E-Discovery Case Examples

• A forensic examination of an ex-employee’s hard drive and cell phone where it is believed they took proprietary information to their next employer
• Expert authentication of a set of ten email, photographs and documents
• Keyword search of two years of email for 6 custodians and their loose and paper files, including attorney review, coding, and production
Medium Sized E-Discovery Case Choices

• Collection choices: forensic imaging (internal or vendor), remote collection of DropBox
• Processing choices: load to simple processing/review tool (desktop or hosted), vendor indexing, filtering, de-dupe
• Review choices: load to review tool (desktop or hosted)
• Production choices: produce from desktop/hosted tool
• Or, a hybrid
Large Sized E-Discovery Case Scenarios

• Remote collection of multiple server shares for large date range (email and files), concept clustering, attorney review for hot documents

• Onsite collection of six computers and cell phones, keyword search, attorney privilege review, production to opposing

• One dozen employees email, filtering and attorney review in response to government subpoena
Large Sized E-Discovery Case Choices

• Collection choices: use internal or external resources to create forensic images, use remote assisted collection when possible

• Processing choices: load to robust processing/review tool (using vendor or internal resources) to indexing, filtering, de-dupe, cluster

• Review choices: load to review tool, use contract reviewers if necessary

• Production options: produce or direct vendor to produce, multiple levels of QC

• Or, a hybrid
Connected Devices

**Smart Phone**
- Fitbit App
  - Mr. Coffee
    - Connect through WiFi to app that brews coffee when the alarm is dismissed

**Mr. Coffee**
- Connect through WiFi to app that brews coffee when the alarm is dismissed

**Smart Car**
- GPS Navigation
- Hands free commands
- Intuitive maintenance checker

**Work PC**
- Email
- Microsoft Office
- Databases
- Servers
- Browsing Activity

**Home Security**
- Viewable/Controllable w/App
- and via port-forwarding on a browser
- Saved to DB through company or on your personal computer/phone/SD card

**Amazon - Echo**
- Always Listening

**Fitbit - Flex**
- Tracks sleep patterns
- Tracks steps
- Silent alarm
- Syncs w/Account

**Samsung - Smart Fridge**
- Scans for RFID
- Syncs w/Smart Phone

**Bluetooth**
- Hands free commands

**GPS**
- Intuitive Navigation

**Security Card**
- RFID Chip that allows access to secure areas
- Records a log of each scan which can be tied to security footage

**Smart Stove**
- Remote start
- Syncs with multiple accounts

AVANSIC
E-Discovery & Digital Forensics

E-Discovery, Security and Social Media
E-Discovery and Security

• “Deepest Darkest Secrets”
• Challenges at every phase of e-discovery
  – Preservation: custody and control
  – Processing: no comingling, secure laboratory at vendor, encryption
  – Review: strong user authentication, auditing and tracking
  – Data storage: insecure file-sharing (Dropbox, etc.)
  – Communication: careful with non-encrypted email

• Each additional layer of security means a reduction in convenience
  – Time
  – Ease of technology use
  – Encryption
What is the Cloud?

• Using a “shared pool of configurable computing resources” (NIST)
  – Gmail (or any other webmail)
  – DropBox or Google Documents
  – Offsite application hosting
  – Your office network

• Types
  – Software
    • Common
    • Use someone else’s software to perform an operation
    • “Software as a Service”
  – Hardware
    • Using someone else’s processing power
    • IE, animation company rendering graphics
Free Data Security - Encryption

• Encoding data/messages so only authorized parties can read them
• Does NOT prevent interception (it actually expects it)
• Not just password protection the stored data is secured
• Every extra security measure introduces a loss of convenience
  – Generally free (BitLocker, 7-Zip AES encryption)
  – Key management, personnel training, small to medium IT burden
• Could become requirement by ABA ethics
HIPAA Case Study

• **Malpractice suit against a hospital, so HIPAA applies**
  
• **Lead attorney…**
  
  – Contacted the firm’s IT to discuss requirements: NIST 800-111 for data at rest, NIST 800-52 or 800-77 for data in motion
  
  – Requested that any productions from any party be encrypted
  
  – Interviewed e-discovery vendors, specifically about encryption and HIPAA BAAs

• **Firm IT and Vendor**
  
  – Made changes in hardware, software and procedure to meet NIST standards
  
  – Vendor created secure FTP and ability to encrypt email
  
  – Vendor offered an online review tool that met the requirements

• **Project Progression**
  
  – Everyone gets BAAs (Business Associate Agreements)
  
  – Vendor received the encrypted drive, processed and loaded to review
  
  – Physically & logically separated this case’s data from all others
  
  – Attorneys reviewed and coded documents
  
  – Vendor created production, encrypted it, sent to the firm
  
  – When case was complete, the firm and the vendor destroyed data per NIST 800-88
Social Media and Cloud Preservation

- Huge amount of personal and corporate information
- Time is of the essence - preserve key data immediately
  - Must be handled as evidence in order to ensure admissibility
  - Some sites have a “self-preserve” feature (Facebook)
- Not easy
  - Some service providers are cooperative, most are NOT!
  - Cloud/synced data can be difficult to locate
- Related mobile data is stored…
  - In the cloud and/or synced to another computer or server
  - On the device itself
  - On-device storage is limited and therefore overwrites quickly
- BYOD issues (Bring Your Own Device)
  - Mobile devices make access easy
  - Purpose is to freely share information
  - Publicly dispersed rather than specifically targeted (i.e., e-mail)
Social Media - Who Owns the Content?

• Individual employees tasked with social media content/posts

• Does company own the profile and any associated posts? Or does the person who posted?
  – Twitter: PhoneDog v. Kravitz – editor-in-chief started a Twitter account for the company then left, claimed the followers and content were his personally, company sued for economic interference, the case is ongoing
  – Eagle vs. Edcomm – Company shut down an employee’s LinkedIn account after she left, court ruled that it did not violate the Computer Crimes and Abuse Act
  – No universal ruling, case-by-case basis
The Internet Has a Memory

• Very difficult to take back something said or shared on the Internet
  – Erasing profiles is expensive and hard
  – Most hosting sites have cached versions of posts and pages
  – Even if those are deleted, anyone who viewed that page may have pieces left on their computer
  – Wayback machine

• Imagine if corporate data was inadvertently exposed or shared
  – Or privileged information
  – Careful, thorough and clear policies
  – Careful control and selection of the individuals who can post on behalf of the company
Conclusion

- Carefully balance risks and benefits
  - Cloud
  - Social Media
  - Portable Devices
  - Computer Use

- Consider yourself, your firm and your client

- Security and privacy are paramount with electronic data

- Increasing security usually means decreasing convenience