



AVANSIC[®]

E-Discovery & Digital Forensics

evidence at your fingertips.

Digital Security

Dr. Gavin W. Manes, Chief Executive Officer

- **Avansic**

- E-discovery and digital forensics company founded in 2004 by Dr. Gavin W. Manes, former Computer Science professor
- Scientific approach to ESI processing
- Strong background in academics and research
- Expert Project Managers – Brad Deavers and Meredith Lee

- **Gavin W. Manes, Ph.D. – CEO**

- Nationally recognized expert in e-discovery and digital forensics
- Frequently published in peer-reviewed journals, magazines, and proceedings
- Presents to attorneys and professional organizations
- Serves as an expert witness

Agenda

- The Problem
- The Challenge
- Solutions

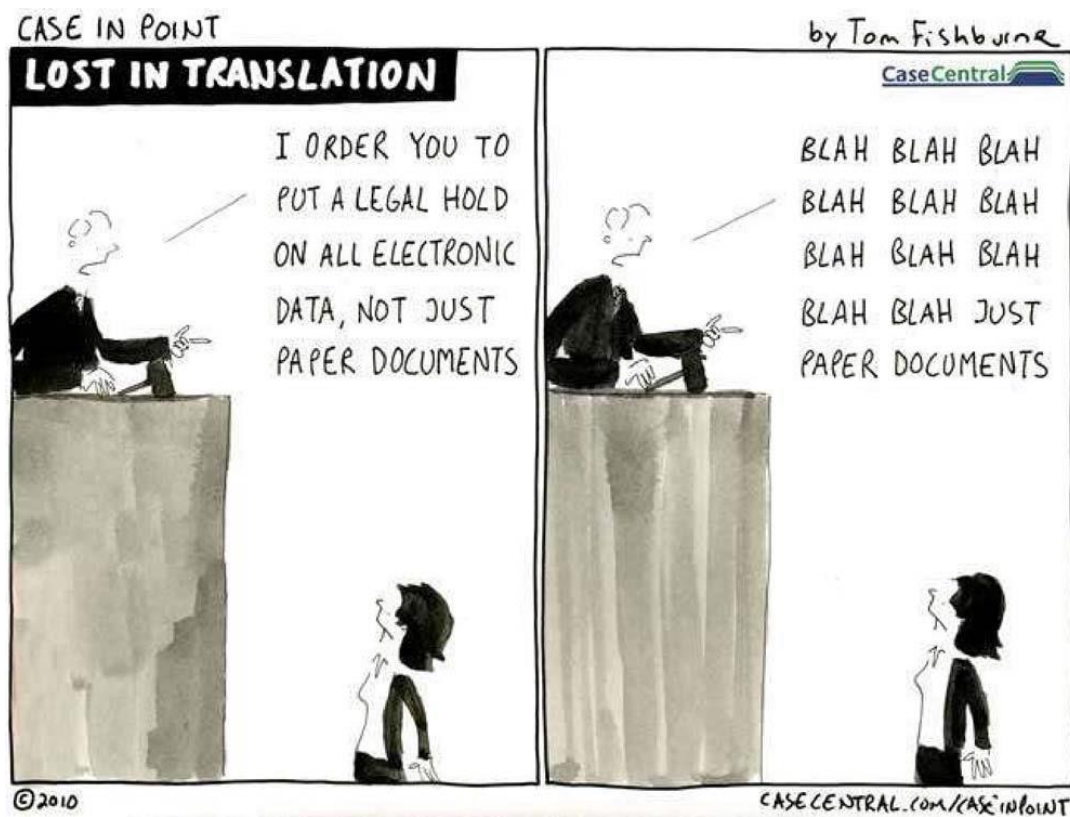


The Problem



- The Unknown
 - Attorneys
 - IT systems
 - Policies and procedures
 - Where's the data?
 - Encryption, passwords
 - Corporations
 - ESI Rules
 - ESI Costs
 - Government
 - Learning to request Natives

Communication and Vocabulary



- Good communication is critical – jargon is dangerous
- Technical terms can be defined MANY different ways

Recent Issues

- **Key Decisions**
 - Zubulake (the beginning)
 - New decisions every day
- **Technology**
 - Cloud [Public/Private]
 - Hacking
 - Encryption
 - Data sizes
- **New Rules**
 - ABA Ethics
 - HIPAA
 - Privileges



Tools in the Industry

- No one tool does everything WELL
- Use a tool for what it's best at – best in class
 - Case management tools
 - Litigation hold
 - Evidence management
 - Trial preparation
 - Collection tools
 - Processing tools
 - De-dupe
 - Clustering
 - Exceptions
 - Review tools
 - Redaction
 - Predictive review
 - Production tools

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

E-Discovery Goals

- Reduce risk and save money
 - Thorough preservation and collection (correct personnel)
 - Thoughtful processing and filtering
 - Review using modern and cost effective review tools (online)
- Why?
 - Human review time is the most expensive and error-prone part of the process
 - Let the computers filter out unresponsive documents using defensible methods
- How?
 - Planning ahead, crafting a strategy
 - Carefully selecting exactly the right vendor for the project
 - Using the appropriate team (including vendor)

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

ESI Processing

IDENTIFICATION & STRATEGY



Data, Custodians,
IT, Standards

AVANSIC ESI PROCESSING

copyright 2013 Avansic, Inc.

for more detail visit

<http://www.avansic.com/ESIProcessing>

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



Loadfiles

Summation[®], Excel[®],
Concordance[®], Format
Conversion



Recovery

deleted, broken,
double-deleted

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



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

Benefits & Challenges

- **Benefits**

- Outsourcing IT
 - Install, update, maintain software
 - Can be cost-effective

- **Challenges**

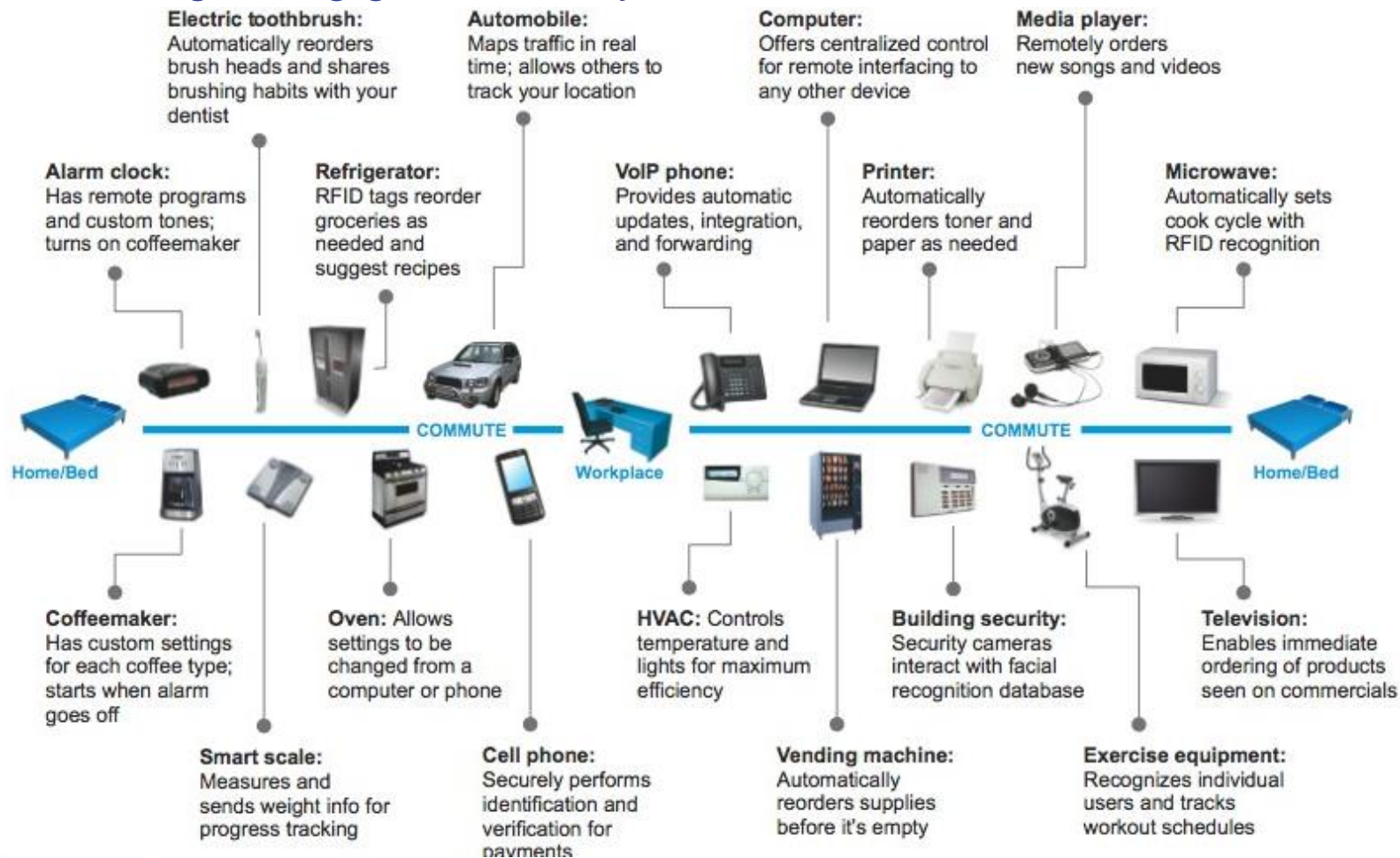
- Privacy & security
 - Confidentiality issues
 - IT may not know the specific needs of legal professionals
 - Physical and remote access considerations
- Disposal of data
 - Protective orders may require certified destruction
- Jurisdiction
 - Cloud facilities may be outside the US

Cloud Considerations

- Evaluate your risks for:
 - Your firm's data
 - Your client's data
 - Opposing party's data
- Then, balance those risks
 - Continuous litigation hold – may be very difficult to use the cloud
 - Dispersed firm and litigation teams – may be worth the risk for the added convenience

Personal Security

Number of connected devices be more numerous than computers at least 5 to 1, growing geometrically.



Legal Considerations

- Dropbox, GoogleDocs and WebDAV (Cloud Storage)
 - Used by most apps to move data from an outside source to the iPad
 - Using cloud storage may create risks to your client's confidentiality
 - ABA Commission on Ethics 20/20 Working Group on the Implications of New Technology "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology"
 - Limited other solutions



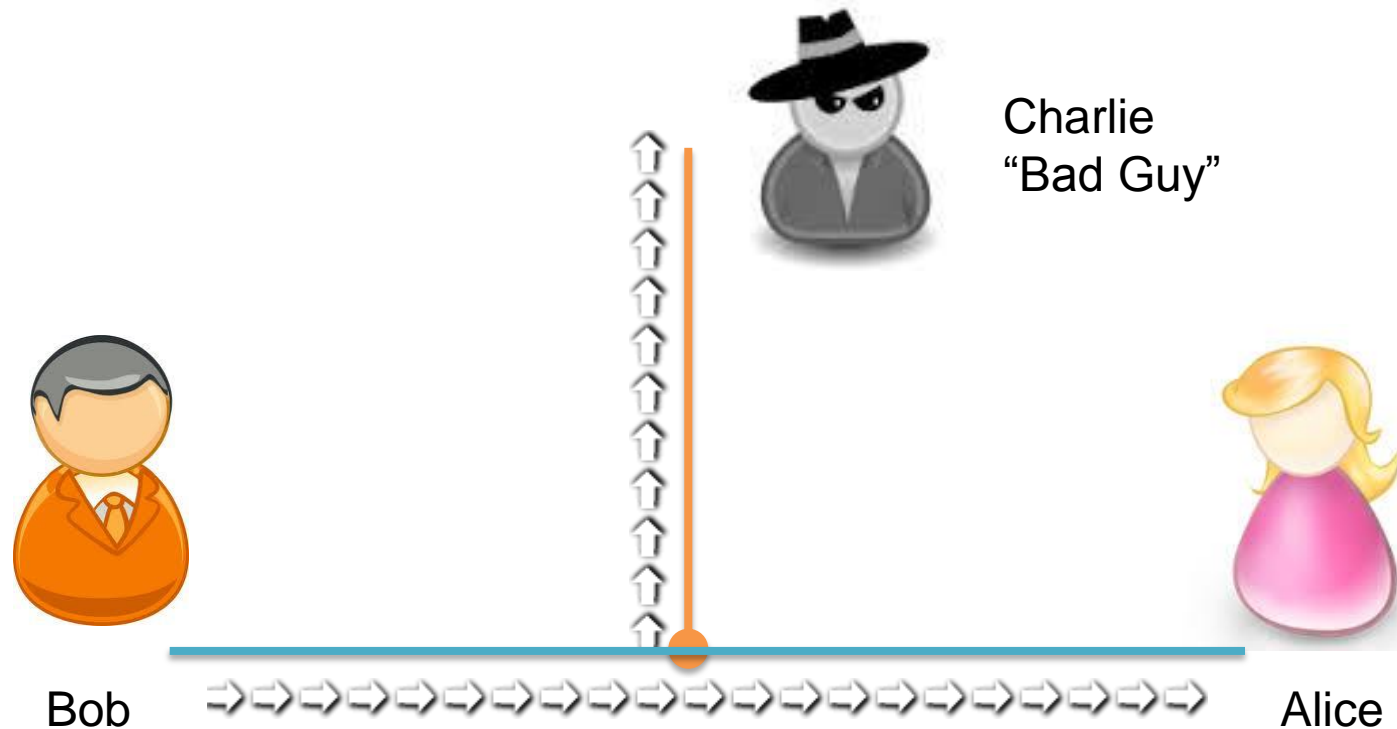
Encryption Basics

- Encoding messages so only authorized parties can read them
- Does NOT prevent interception
- Not just password protection
 - Boot from thumb drive/CD
- Every extra security measure introduces a loss of convenience
 - Additional software, key management, personnel training, IT burden

Plain Text Communication

No.	Time	Source	Destination	Protocol	Info
1096	48.512009	129.244.37.171	129.244.73.33	TCP	1037 > 110 [SYN] seq=151274019
1097	48.512682	129.244.73.33	129.244.37.171	TCP	110 > 1037 [SYN, ACK] seq=1811
1098	48.512737	129.244.37.171	129.244.73.33	TCP	1037 > 110 [ACK] seq=151274019
1099	48.545471	129.244.73.33	129.244.37.171	POP	Response: +OK QPOP (version 3.
1100	48.545704	129.244.37.171	129.244.73.33	POP	Request: USER Forensics
1101	48.546267	129.244.73.33	129.244.37.171	TCP	110 > 1037 [ACK] seq=181152723
1102	48.546798	129.244.73.33	129.244.37.171	POP	Response: +OK Password require
1103	48.546901	129.244.37.171	129.244.73.33	POP	Request: PASS thisishepassword
1104	48.641098	129.244.73.33	129.244.37.171	TCP	110 > 1037 [ACK] seq=181152727
1322	58.543602	129.244.73.33	129.244.37.171	POP	Response: -ERR [AUTH] Password

Encryption Example



We should settle for \$500K but only offer \$200K now

4t;93qhg5;l8q3'u9gy7q13941yh4'gq3whrb9'3qh5ge

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 opposing be encrypted
 - Interviewed e-discovery vendors, specifically about encryption
- Firm IT...
 - made changes in hardware, software and procedure to meet these
 - Created secure FTP and ability to encrypt email
 - Implemented two factor authentication

Case Study Con't

- Vendor

- Had experience with data containing PHI
- Quickly and articulately outlined their procedures
- Offered an online review tool that met the requirements

- Project Progression

- 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

**Your Computer
Might Be Infected
With Viruses
And/or Adware!**

**Click Here To
Make Sure It Is**

We infect your PC for *FREE*
AddMalWareNOW.com

Ransomware Hack

The image shows a screenshot of the CryptLocker ransomware interface. It consists of two main windows. The left window, titled 'CryptLocker', has a red background and a blue shield icon with a white cross. It displays the message 'Your personal files are encrypted!' and provides instructions on how to obtain the private key for decryption. A timer shows '71:59:52' remaining. The right window, titled 'Payment for private key', also has a red background and features a Bitcoin logo. It prompts the user to choose a payment method (Bitcoin is selected) and provides a Bitcoin address and transaction ID for payment. A 'PAY' button is visible at the bottom right of the interface.

CryptLocker

Your personal files are encrypted!

Your important files **encrypted** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **8754-2018** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.


Private key will be destroyed on
9/20/2013
5:54 PM

Time left
71:59:52

Next >>

Payment for private key

Choose a convenient payment method:
Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address
1KP72fBmh3XBRfuJDMn53APaqM6fMRspCh and specify the transaction ID, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

2 BTC

<< Back PAY

Cloud and Social Media Data

- Adds a new dimension to BYOD
 - Mobile devices make access easy
 - Purpose is to freely share information
 - “Everybody’s doing it”
 - Publicly dispersed rather than specifically targeted (i.e., e-mail)
- Huge amount of personal and corporate information
- BYOD leads to BYO-CLOUD
 - Most cloud backup services are automatic and use personal accounts
 - iCloud
 - Gdrive
 - SkyDrive

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



AVANSIC[®]

E-Discovery & Digital Forensics

evidence at your fingertips.

avansic.com

Corporate Office

First Place Tower, Suite 1800

15 E. Fifth St, Tulsa, OK 74103

Gavin W. Manes, Ph.D.

gavin.manes@avansic.com