Cyber Security

Criminal electronic discovery

Digital privacy

Big data

Keyword search

C 01000011

N 01001110

M 01001101

I 01001001

BYOD

Amended FRCP (Dec. 2015)

Litigation strategy

Supreme Court 2014 term

Cloud Computing

Agenda for 2014 District Conference

- Electronic Discovery
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

E-Discovery

Litigation Strategy

What is Electronic Discovery

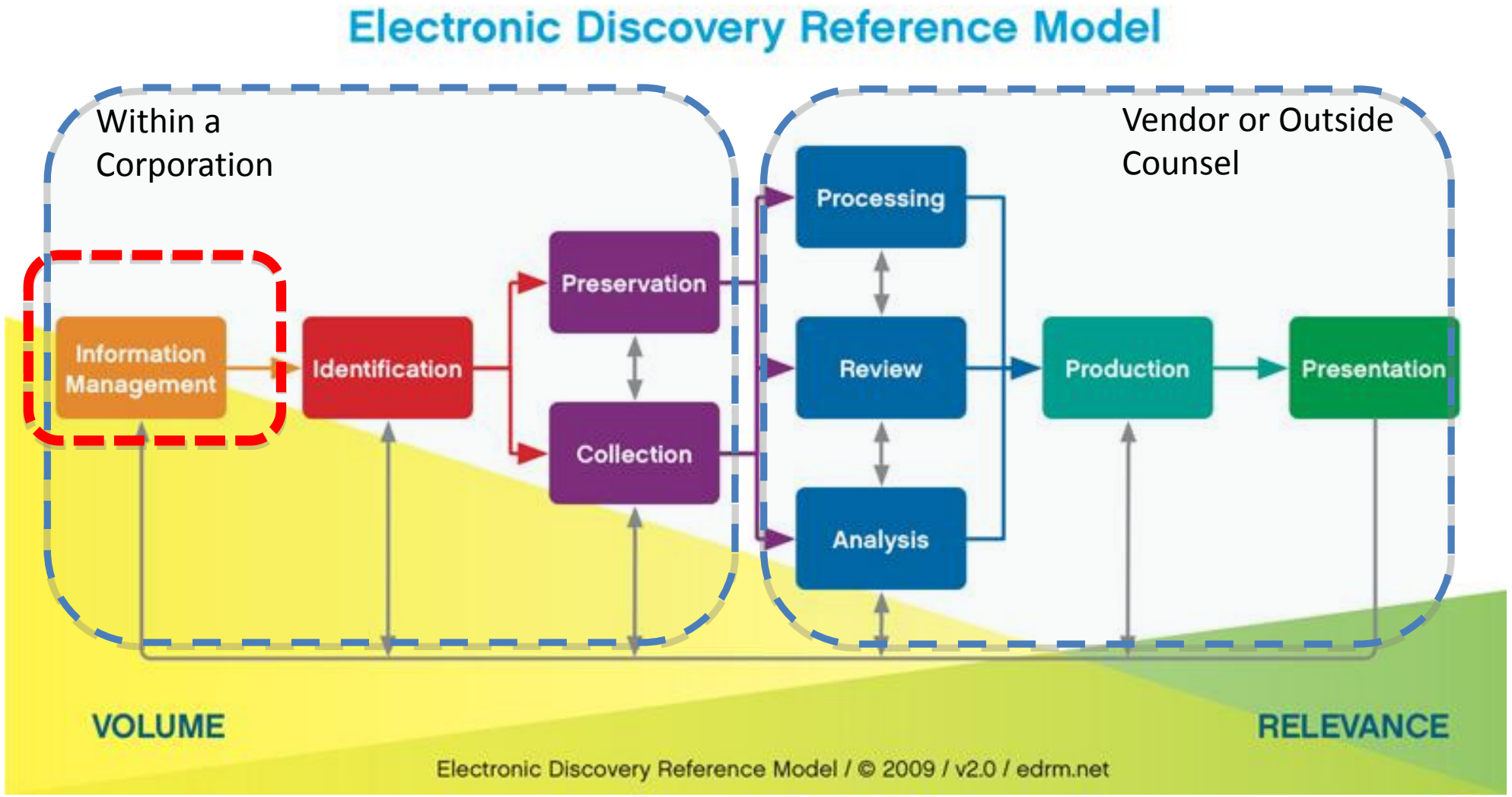
Electronic Discovery is the process of identifying, collecting, preparing, reviewing, and producing Electronically Stored Information (ESI) during the legal process. ESI is not paper in electronic form

Why lawyers hate e-discovery? The information feels ephemeral. The mechanics behind ESI confuse us. Not literate in IT language or practice.

Why lawyers tend to dislike e-discovery?

- **Horror stories….**
- **Sanctions against Client even when the client lost/destroyed documents by accident**
- **Sanctions against the Lawyers even when the lawyer made reasonable efforts**
- **Entirely new standards for handling information that no one anticipated.**
- **Unstructured Data**
- **Dusty Data/Dark Data**
- **Highly inconsistent rulings**

Electronic Discovery Process Flow



If a tree falls….

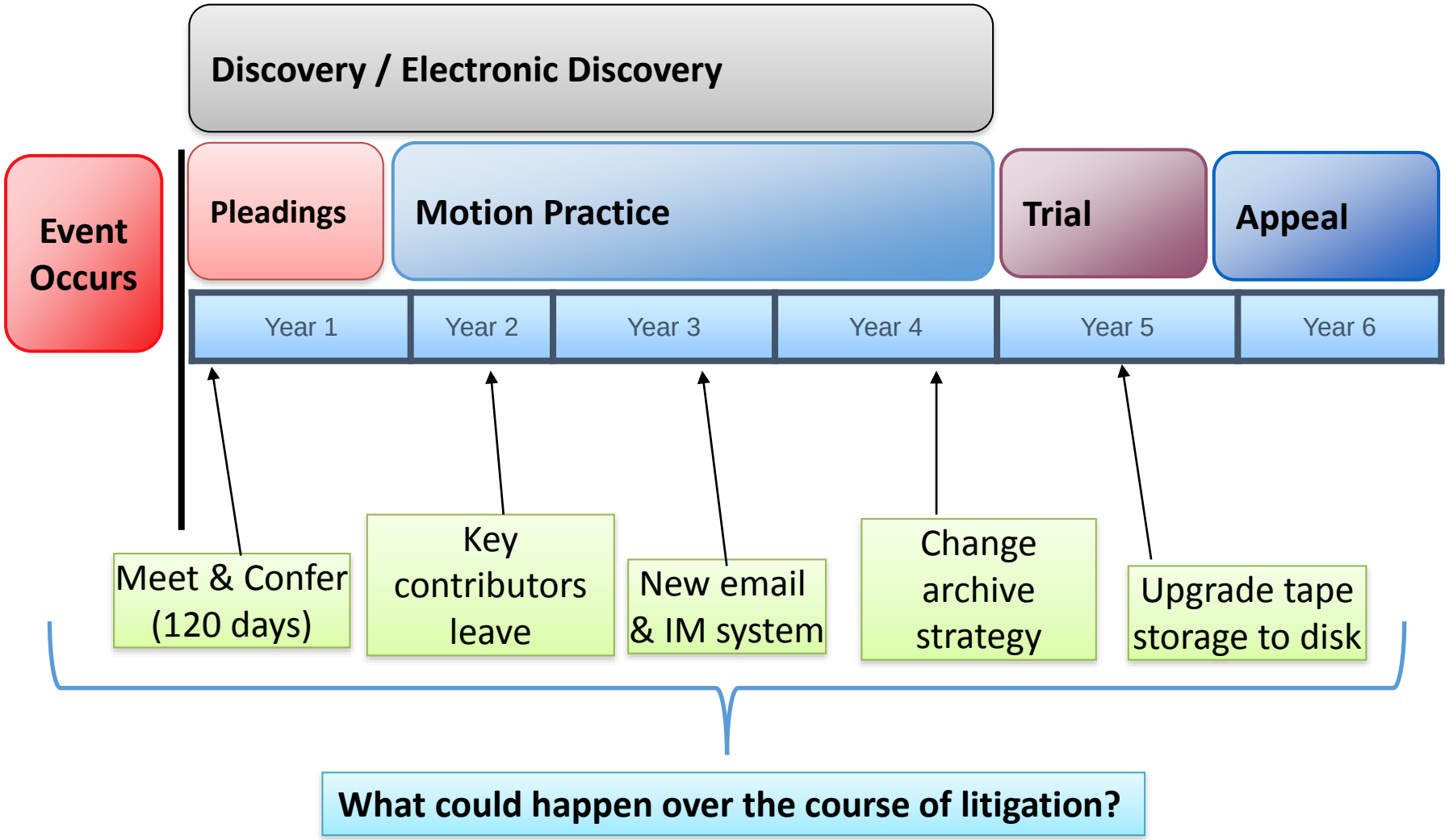
Lawyers often reference millions of documents to be collected, but most of them have little if any value and mislead the court.

Basic math shows the absurdity.

Number of Docs		Time
20,000,000.00	1825	Days
	1440	Minutes/day
	2,628,000.00	Total Minutes

7.61 Docs/min

A Litigation Timeline



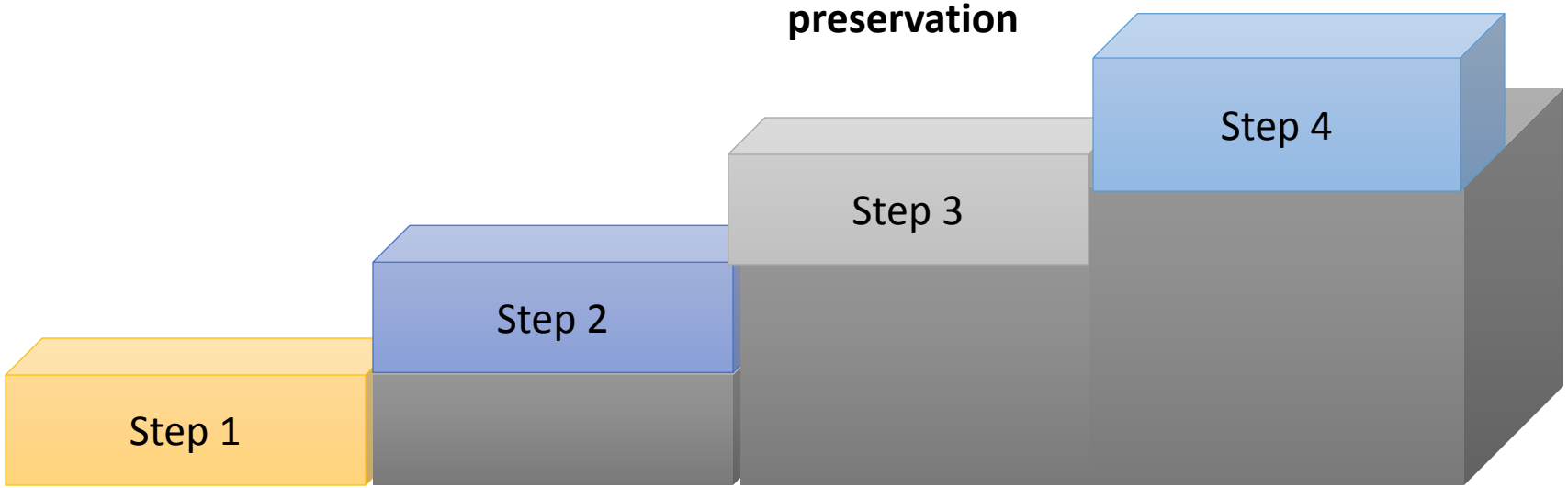
Steps of Discovery.

The Overview – Game Plan

Litigation hold, do you have the right tools and custodians in-place to effectuate a litigation hold.

Scheduling of IT and/or **Custodial Interviews**, do you know the repositories of ESI, best way to collect ESI, and **ensure preservation**

Review preservation process and strategy and prepare for **Collection** of ESI and paper documents.



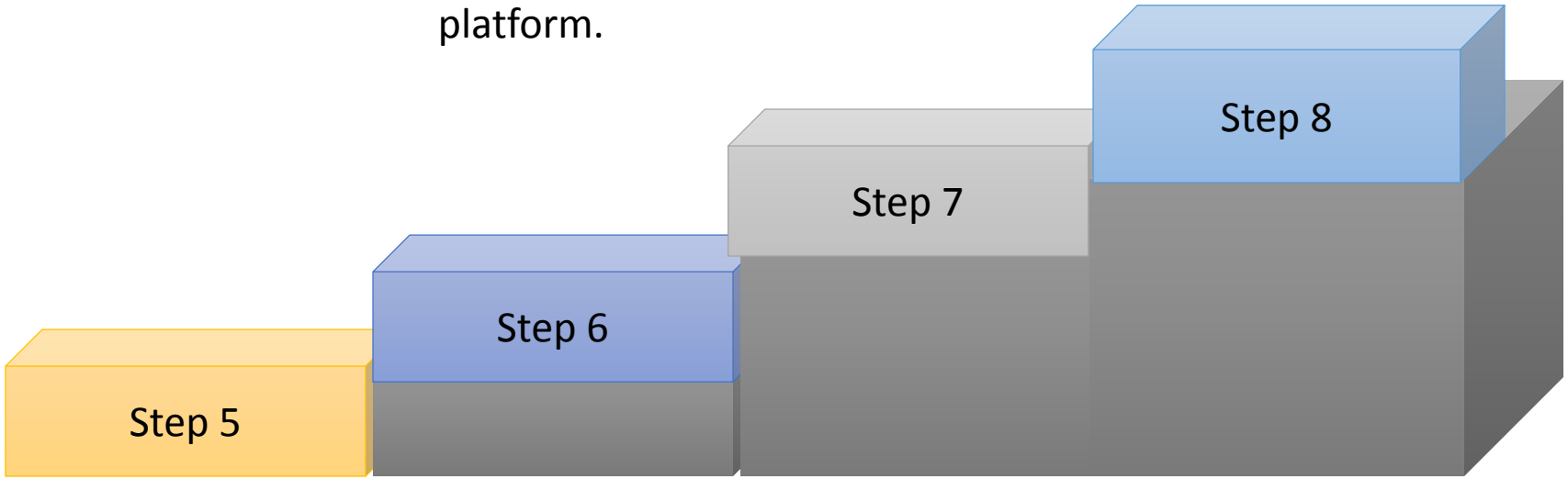
Steps of Discovery.

Collect the ESI and hard documents.

Cut it down, using ECA, keyword, and predictive coding and upload to review platform.

Review document in native and code for responsiveness and issues (e.g., redaction, privilege, and etc.)

Production, depends if ESI protocol was created and executed by parties and etc.



Current State of Fed. R. Civ. P

but changes are coming in 2014….

Fed. R. Civ. P. (2006 Amendments)

Federal Rule of Evidence 502(b): Limitations of Privilege Waiver.

The definition of what is discoverable.

Fed. R. Civ. P. (FRCP) 26(a)(1), 33, and 34;

Dealing with ESI early.

FRCP 16(b), 26(a), 26(f) and Form 35;

FRCP Amendments in more detail

Designating the format of ESI:	• FRCP 34(b) and FRCP 45;
Discovery from sources that are not reasonably accessible:	• FRCP 26(b)(2);
Post-production claims of privilege:	• FRCP 26(b)(5);
Interrogatories and production requests:	• FRCP 33, 34(a), and (b).
"Safe Harbor" for inadvertent spoliation:	• FRCP 37(e);
Subpoenas	• FRCP 45.

FRCP 26(f) – Meet + Confer

Requires that all parties confer "as soon as practicable—and in any event at least 21 days before a scheduling conference is set" to:

- Discuss the nature and basis of their claims and defenses;
- discuss the possibilities for promptly settling or resolving the case;
- arrange for the disclosures required by Rule 26(a)(1);
- discuss any issues about preserving discoverable information; and,
- develop a proposed discovery plan.

Preparing for 26(f) Conference

- Issuing the Litigation Hold
- Identify and Speak with Key Players
- Understanding the Client's Systems
- Understanding the Client's Systems - *Backups*

The parties should be prepared, prior to the meet-and-confer discussions, to discuss:

- The specific data sources in their respective electronic systems.
- The reasonableness of e-discovery of these data sources.
- Stipulations regarding ESI discovery plans that encompass an evaluation of the "proportionality factors" (an evaluation performed by the parties themselves at the outset of the discovery phase).

FRCP Critical Discovery Decisions Come Early

- Rule 16 Conference Order
  - ASAP but at least w/in 90 days of appearance of defendant or 120 days from service of complaint.
- Rule 26(a) disclosures of ESI
  - At or w/in 14 days of 26(f) conference unless a different schedule per stipulation or order.
- Rule 26(f) Conference Among Counsel
  - ASAP but not later than 16 days before Rule 16 conference or issuance of scheduling order.

FRCP 26(a) Initial Disclosures

FRCP 26(a)(1)(A)	• Witnesses, may need to include e-evidence custodian(s).
FRCP 26(a)(1)(B)	• ”a copy of, or a description by category of, all documents, electronically stored information….that the disclosing party may use to support its claims or defenses”
FRCP 26(a)(2) Federal Expert Witness Disclosures	• Witness must prepare and sign written report; Opinions and bases; Data considered; Exhibits; Qualifications, including publications past 10 years; Compensation; Prior cases in past 4 years, trial or deposition

FRCP 33 (Interrogatories to Parties)

Expressly provides that an answer to an interrogatory involving the review of records should involve a search of electronically stored information.

FRCP 34(a) Scope

Any party may serve on any other party a request (1) to produce … **electronically stored information –** (including writings, drawings, graphs, charts, photographs, **sound recordings, images**, and other **data or** data compilations **stored in any medium** from which information can be obtained ….

FRCP Rule 34(b)

Rule 34(b).

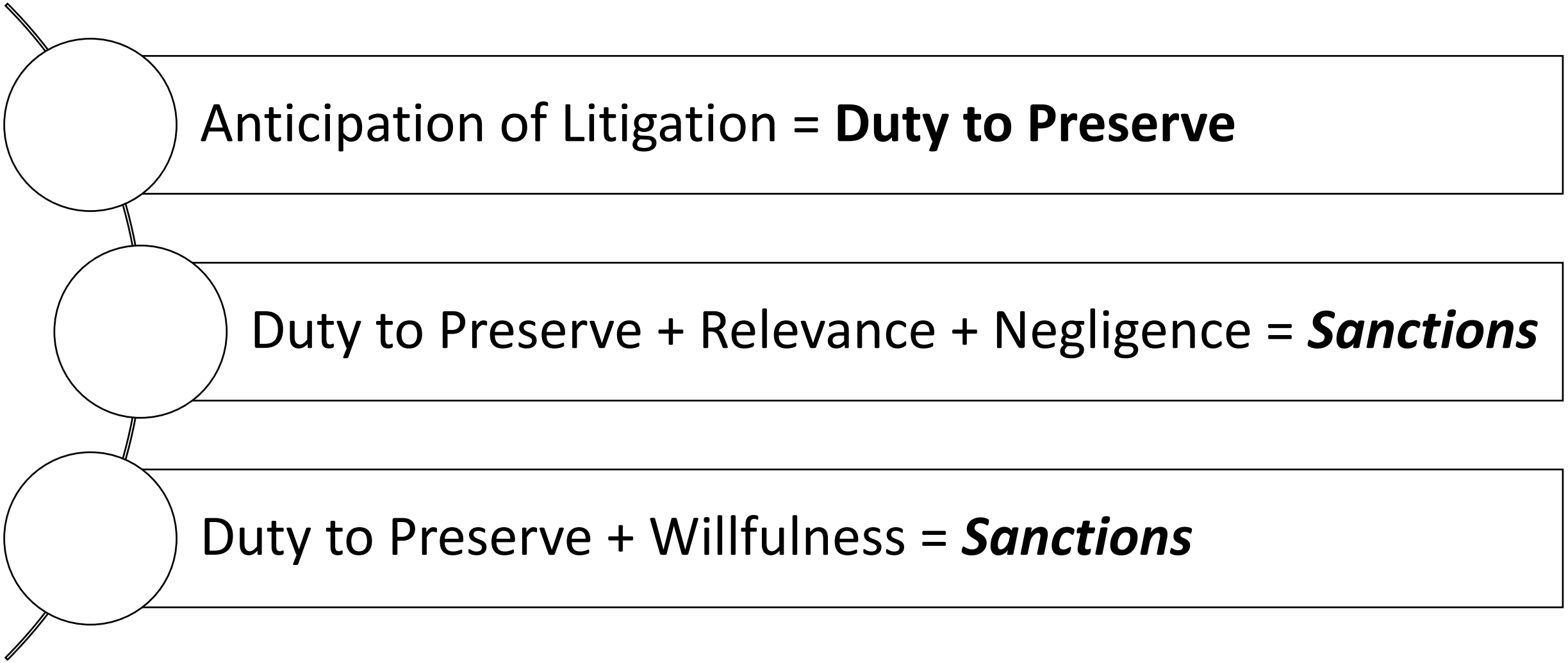
- **The request may specify the form or forms in which electronically stored information is to be produced**
- FRCP 34(b) authorizes demanding party to "specify the form or forms in which [ESI] is to be produced"; subject to challenge. Per Advisory Note, can specify different forms for spreadsheets and documents.

Rule 34(b)(ii).

- If a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable

E-Discovery Penalties

Significant responsibilities and the potential for sanctions



E-Discovery Penalties….

Among other things.

- Deeming Facts Admitted (FRCP 37(b)(2)(A))
- Precluding Evidence (FRCP 37(c)(1))
- Striking Privilege Assertions (FRCP 26(b)(5))
- Striking Designated Witnesses (FRCP 37(c)(1))
- Monetary Sanctions (FRCP 37(b))

Court Sanctions for Retention Policy

FROM THE JULY 2009 ISSUE OF INSIDECOUNSEL MAGAZINE • SUBSCRIBE!

Court Sanctions Company for Retention Policy

BY CHRISTOPHER DANZIG
July 1, 2009 • Reprints

2

Adams filed a motion in *Phillip M. Adams & Associates v. Dell Inc.*, accusing ASUS of destroying evidence that showed its employees had used his technology illegally. During discovery, ASUS hardly turned over anything, which led Adams to suspect spoliation.

In the past, this strategy has been acceptable to judges, as long as a system for preservation kicks in when litigation is anticipated. But that's where the case gets confusing. Nuffer slammed ASUS for not triggering its document preservation plan when it should have anticipated litigation based on other lawsuits happening in the industry.

Failure to retain emails can have a drastic impact on the case and the outcome.

Importance of a Litigation Holds

Apple v. Samsung Sanctions Highlight Importance of Understanding Litigation Holds

AUGUST 2012 BY WILL HELOU

TENNESSEE BUSINESS LITIGATION NEWSLETTER

The sanctions recently levied against Samsung in its patent infringement dispute with Apple serve as a potent reminder that understanding data and document preservation requirements is imperative.

A party has a duty to preserve all evidence, including electronic documents and data that it knows or should know is relevant to any present or future litigation. *See John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008). The filing of a complaint clearly triggers the duty to preserve, although a demand letter or other pre-litigation letter can provide sufficient notice. *See Nacco Materials Handling Group, Inc. v. Lilly Co.*, 278 F.R.D. 395, 402-03 (W.D. Tenn. 2011). Although a preservation letter or court order certainly may clarify the scope of obligations, neither is required for a finding that a party was on notice of pending litigation.

Simple Steps can save you and your clients a fortune and headache.

Don’t Loose Because You Fail to Ask

TR Investors v. Genger, Delaware Chancery Court

Genger deleted the files stored in the unallocated space, meaning the files were already deleted. Nonetheless, the Court:

- Sanctioned Genger $3,000,000.00
- Shifted the burden.

Lessons

- Preservation in good faith is key.
- **Ask** the court if you have doubts.
- Do not litigate the discovery rather than the case.

Be careful what you ask for…

LAW & FORENSICS

A to Z Kosher Beef v. Empire Kosher Poultry

A large corporation - requested expedited discovery. The opposing litigant was a small company. End-result settlement in favor of small company.

Lesson

- Make sure when your Client is a large corporation they are ready for massive effort if seeking expedited discovery.
- Generally, extremely high cost to comply with expedited discovery.
- Counsel will receive little compassion from the court.

…since you may just get it.

Trust but Verify

United Central Bank v. Kanan Fashions (2011)

- Counsels' instructions for preservation to Client went unheeded, resulting in sanctions.
- Documenting efforts gave Counsel credibility.

Lesson:

- Partners at onset of case to liaise with the Client's information technology team
- Document your efforts
- Partners should utilize checklists, including:
  - Checklist for discovery conference
  - Discovery checklist
  - Computer-use policy checklist

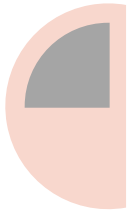
Metadata and Why It May Be Important in a Lawsuit

- Classic e-mail metadata fields
  - From, To, Subject, Date, cc, bcc, Text of email
  - Date and time e-mail and/or attachment opened
- 50-60 other types of fields are available
- Embedded data (e.g., Excel formulas, Word Processing prior versions)
- Expensive to manage and produce; relevance depends on the nature of your case.

How to issue a Litigation Hold

Identify:

- Categories of documents to be preserved
- Time period. Business units effected
- Sources subject to the hold (e.g., backup tapes, home computers)
- Exceptions to routine procedures (e.g., suspension to routine deletions)



Issue to:

- Key players, their staffs, pertinent department heads and, IT personnel responsible for pertinent systems.

Follow up:

- Send regular reminders to key players and departments
- Have HR and IT provide notice of pertinent personnel changes.

Document the steps taken

- Write it down

Predictive Coding…future is now.

Predictive Coding

- Predictive coding (aka: Technology Assisted Review TAR, intelligent review, and computer assisted review) has the most potential to modernize document review practices but predictive coding is used primarily in big cases.
- Studies show that predictive coding can cut review time and costs in half or more.

Adoption Barriers

- Concern they will replace lawyers
- Concern about the defensibility
- Lack of knowledge
- Technology and Best practices are not yet Standardized.

Top Ten Tips

1. **Do a little upfront and save a bundle downstream:** Create discovery plan with clients at the start of litigation.
2. **Glass house dilemma:** Don't ask for sanctions or relief if your not 110% sure you won't be called to task.
3. **Horses mouth:** Identify sources of discoverable information and speak directly with key players in litigation as well as IT personnel.
4. **Trust but verify:** Verify preservation is occurring and always document you verified and informed Client of preservation requirement.
5. **Talk before 26(f):** Discuss systems with your client before 26(f) and continuously communicate discovery obligations to client -- meaningful discussion with client and other attorneys; keep all well informed

Top ten tips.

6. **Talk to the Techies:** Conduct custodian interviews – See Daniel Small v. University Medical Center Case No. 2:13-cv-00298-APG-PAL.
7. **Ask before you Act**: Always ask the Court if you are not sure the court and closely monitor process and reiterate instructions for litigation hold and monitor compliance
8. **Don't let the blind lead the blind: Do** not let your client self-collect unless it can be duplicated and make sure your client has segregated and is safeguarding of archival media (backup tapes) and tell the other side if you have issues.
9. **Don't litigate the discovery:** Dialog and cooperation with opposing counsel will be more fruitful than fighting.
10. **You the boss**: Take control of document production do not let your client control it – collaborate is ideal.

Questions

Answers

Agenda for 2014 District Conference

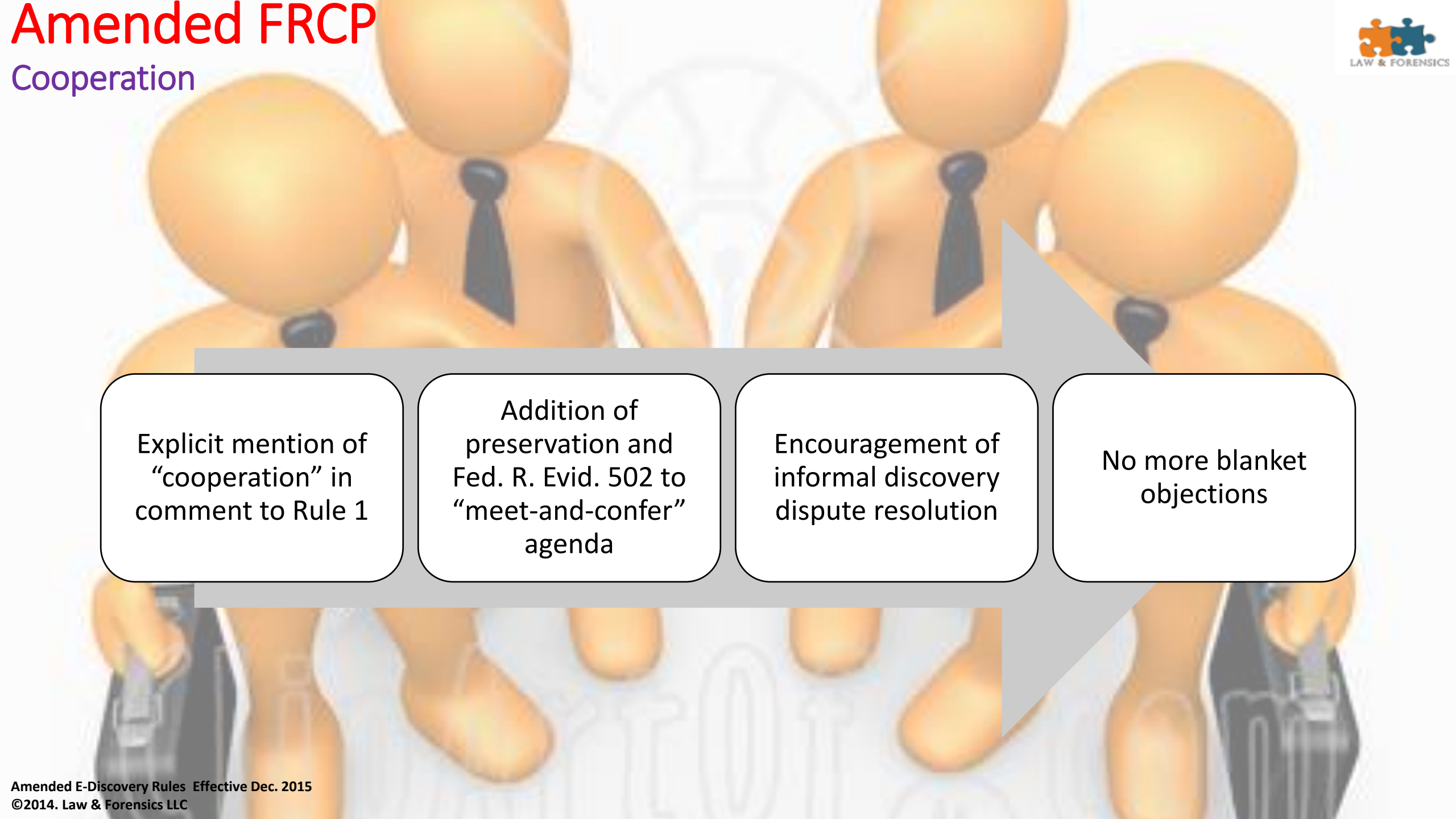
- Electronic Discovery
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

December 15, 2015

Amended
E-Discovery Rules
Effective Dec. 2015

Amended FRCP

Cooperation



- Explicit mention of “cooperation” in comment to Rule 1
- Addition of preservation and Fed. R. Evid. 502 to “meet-and-confer” agenda
- Encouragement of informal discovery dispute resolution
- No more blanket objections

Amended FRCP

Rule 26(f)(3)

(3) ***Discovery Plan.*** A discovery plan must state the parties' views and proposals on: * * *

(C) any issues about disclosure, ~~or~~ discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;

(D)any issues about claims of privilege or of protection as trial-preparation materials, including — if the parties agree on a procedure to assert these claims after production — whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;

Amended FRCP

Rule 16(b)(3)

New Rule 16(b)(3)(B)(v) allows court to require a conference before any party moves for a discovery order

Amended FRCP

Rule 34(b)(2)(B) and Rule 34(b)(2)(C)

(B) *Responding to Each Item*. For each item or category, the response must either state that inspection and related activities will be permitted as requested or state ~~an objection to the request~~ the grounds for objecting to the request with specificity, including the reasons. * * *

(C) *Objections.* An objection must state whether any responsive materials are being withheld on the basis of that objection. * * *

Amended FRCP

Rule 26(b)(1) and 26 (c)

LAW & FORENSICS

Key Points..

Proportionality factors moved up from Rule 26(c) to 26(b)(1); “Subject matter” discovery gone

Proposed amendment to Rule 26(c) explicitly allows for allocation of discovery expenses

Various amendments compress the pretrial timetable

Amended FRCP

Rule 37(e) (continued)

(2) Upon a finding of prejudice to another party from loss of the information, order measures **no greater** than necessary to cure the prejudice.

Questions

Answers

Agenda for 2014 District Conference

- Electronic Discovery
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

Challenges of Search

Digital Challenges	Volatile | Portable | Alterable |Distributed | Persistent | High volume | High quantity
	Favorite targets for investigations: E-mail & attachments | Instant messages | Document Metadata | Voicemail & Unified Messaging data | Portal & web content (blogs, wikis, etc.)
	Find the 'smoking gun' (i.e., conclusive evidence)
	Prove there is no 'smoking gun'
Challenges in Volume	Moving from large volumes of data to relevant evidence
	Preservation of evidential weight, chain of custody & defensibility
	Maintaining transparency & validation of process
	Ensuring accuracy & completeness of evidence
	Proving reliability & trustworthiness of evidence

How many documents do your keywords pass through?

1 hard drive + 12 monthly backups	13
3 internal recipients	39
5 drafts reviewed by recipients	195
E-mail used to circulate drafts and final of the document	Over 1,000

Developing a Search Strategy

- Think about what documents you want
- Develop relevant KEYWORDS– *not subject headings, not concepts*
  - Alternative ways to express it: common, technical, acronyms
  - Alternative spellings
  - Related terms
  - Synonymous terms

Search is Imperfect….

No magic bullet

- Language is imperfect/ambiguous
- People make mistakes (typos)
- Machines break and can not recognize all text
- Foreign languages
- Non-textual ESI (iPhone, movies, pictures)
- Lack of helpful metadata
- Culture – hoodie v. jumper
- Context – Dyslexia/dyscalculia/mobile/email/web

Challenges of Search

Am I really discovering everything?

- Double quoting: "did I do that"
- Noise words: 'a', 'and', 'the', 'from', and 'because'
- Boolean operators in phrases
- Wildcard specifications: fail* & spec*
- Case sensitivity: a v. A.
- Truncation & Stemming specifications
- Cultural: jargon
- Context: mobile/email/document

Am I looking in the right places?

- Consideration of target data sources
- Appropriate sources
- Character coding of the text – UTF-8, UTF-16, CP1252, Unicode/WideChar etc.
- Special character sets

Am I looking for the right things?

- Is my scope defined adequately?
- What headers am I searching?
- Am I using correct operators and syntax?

Check List for Running Effective Search

Apply common sense and cooperation

Engage in-house technology people early on to reduce cost and lower chance of error.

Take control of the process early.

Questions

Answers

Agenda for 2014 District Conference

- Electronic Discovery + Litigation Strategy
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

Cyber Security

Bench. Bar. Clients

We All Know About the Headlines…

The New York Times

January 30, 2013

Hackers in China Attacked The Times for Last 4 Months

NICOLE PERLROTH

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and security experts have expelled the attackers and kept them from breaking back in.

THE NATIONAL LAW JOURNAL

February 1, 2013

A Cybersecurity Blanket: New Executive Order Means a Broad Review for Lawyers, Clients

TODD RUGER

The federal government's new push to bolster cybersecurity will create an array of legal questions and potential pitfalls for companies in the coming months.

The New York Times

February 1, 2013

Twitter Hacked: Data for 250,000 Users May Be Stolen

NICOLE PERLROTH

Twitter announced late Friday that it had been breached and that data for 250,000 Twitter users was vulnerable.

The company said in a blog post that it detected unusual access patterns earlier this week and found that user information — usernames, e-mail addresses and encrypted passwords — for 250,000 users may have been accessed in what it described as a "sophisticated attack."

CEOs/Boards are no longer ignoring Technology Risks

- **Information and Technology Risk is an enterprise-wide issue. Specific types of risks organizations are facing include:**
  - Connected IT infrastructure exists in an environment that is **increasingly under threat** against unauthorized access or disclosure of sensitive data and attacks originating from cyber-criminal groups and hackers.
  - Increase in **Privacy and Security regulatory mandates** in recent years, as well as expected changes in upcoming years.
  - Boards are no longer willing to accept the **risk that technology can pose** to the business.
  - Growing demand by business leaders to understand **how security integrates with privacy** ("what" data is sensitive to the business) and security ("how" they protect the data deemed sensitive).
  - Increase in threats and vulnerabilities to **sensitive data and corporate assets**.
  - Businesses continue to struggle to **maintain accountability to their stakeholders** and establish effective strategies and standards for security risk management and privacy control activities.

"Securing cyberspace is one of the most important and urgent challenges of our time."

~Senator Jay Rockefeller, Chairman of the Senate Commerce, Science and Transportation Committee

"… There are more than 10K identity-fraud rings in the U.S."

"ID Fraud is Now Organized Crime", By Taylor Armerding, December 2012/January 2013, CSO magazine

"New Ponemon Study Finds Healthcare Breaches Rise 32 Percent"

From IAPP Daily Dashboard <publications@www-privacyassociation.ccsend.com> , 29-Feb-2012

Download: The Ponemon Institute's "**Study on Patient Privacy and Data Security", December 2011**, sponsored by ID Experts at http://www2.idexpertscorp.com/ponemon-study-2011/

Lawyers and Clients

The technology and amount of confidential data that an law firm relies upon to conduct its business can also significantly increase its vulnerability to cyber security threats – any of which can result in significant out-of-pocket and reputational costs that can devastate the bottom line.

A lawyer has duty of privacy and confidentiality to their client.

While the Lawyers Professional Liability policy may address some risk regarding this duty, there are additional risks – and costs – firms may face today.

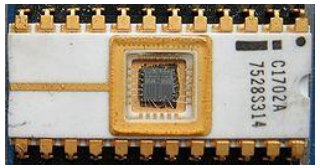
Real world vulnerabilities

Where Do We Find Embedded SW?

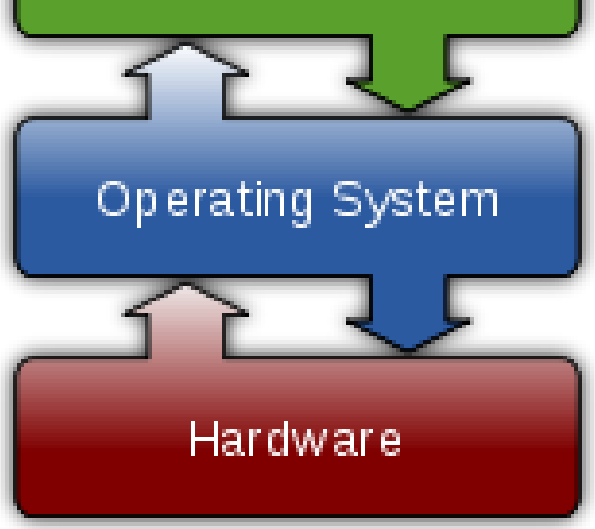
1. Commercial Devices
   - Smart Phones, Cars, Appliances
2. Enterprise Systems
   - Printers, Routers, Switches, Firewalls, VOIP Phones

3. Tactical Systems
   - Weapon Systems, Training & Maintenance Devices

4. Critical Infrastructure
   - **Nuclear Plants, Power Plants, Access Controls**



Erasable Programmable Read Only Memory (EPROM)



Field-Programmable Gate Array (FPGA)

Social Media Risk Deep Dive

- **Malware and viruses**
  - Data leakage/theft
  - “Owned” systems (zombies)
  - System downtime
  - Resources required to clean systems
- **Brand hijacking**
  - Customer backlash/adverse legal actions
  - Exposure of customer information
  - Reputational damage
  - Targeted phishing attacks on customers or employees
- **Lack of control over content**
  - Enterprise’s loss of control/legal rights of information posted to the social media sites
- **Customer service dissatisfaction**
  - Customer dissatisfaction with the responsiveness received in this arena, leading to potential reputational damage for the enterprise and customer retention issues.

How Does It Happen?

LAW & FORENSICS

Targeted Attack

Anonymous gets angry; Competitor hack

Intentional Employee Theft

i.e. Data sent offsite

Equipment Theft

i.e. Laptops or mobile device stolen from vehicle

Employee Error

i.e. Emails oops

Scenario 1: Lost Blackberry

An accountant forgets an unencrypted Blackberry in an airport restaurant.

It is never recovered.

It is late at night on a weekend and the Blackberry is not remotely wiped for 2 days.

The accountant has 8,000 emails and some contain protected financial information.

Scenario 2: Cyber Theft

SQL Injection/Website

On a "black hat" website, Mary Jane learns how to write an SQL Injection script that gets her access to an accountant's databases through their website.

Download from website

She is able to access and download over the Internet names, addresses and Social Security numbers of 500 of the firm's clients.

Breach occurs

As required under State breach notification laws, the firm notifies their affected clients, incurring $150,000 in notification and related crisis management expenses.

Scenario 3: Inside Job

Prior to dismissal for cause, a disgruntled techie installs a logic bomb into the firm's computer system.

Some time after departure, the logic bomb began systematically corrupting critical data.

The firm identified the root cause and quickly quarantined the corrupted data. However, it took several months to restore the data and resume normal business operations.

Cyber Security Issues facing Lawyers and Clients

Plan before disaster strikes.

What questions should be answered?

Has your firm ever experienced a data breach or system attack event?

- Some studies show 80-100% of execs admitted to a recent breach incident

Does your organization collect, store or transact any personal, or financial or health data?

Do you outsource any part of computer network operations to a third-party service provider?

- Your security is only as good as their practices and you are still responsible to your customers

Do you use outside contractors to manage your data or network in any way?

- The contractor, SP, Biz partner is often the responsible party for data breach events

What questions should be answered?

LAW & FORENSICS

Do you partner with entities and does this alliance involve the sharing or handling of their data (or your data) or do your systems connect/touch their systems?

- You may be liable for a future breach of their network and/or business partners often require cyber risk insurance as part of their requirements

Does your posted Privacy Policy actually align with your internal data management practices?

- If not you may be facing a deceptive trade practice allegation

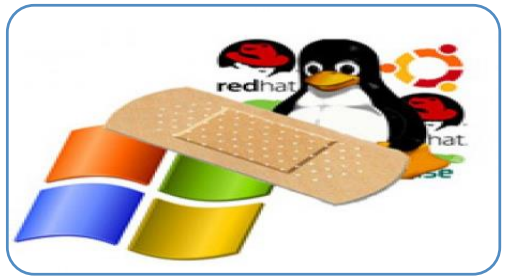
Has your organization had a recent cyber risk assessment of security/ privacy practices to ensure that they are reasonable and prudent and measure up with your peers?

- Doing nothing is a plaintiff lawyers dream. It is vital for the Risk Manager and Privacy Manager to know if your practices are reasonable, in line with peers and the many regulations

Other common weak spots.

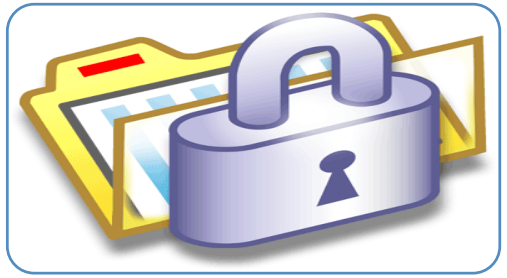
IDS or ‘Intrusion Detection Software’ (bad guy alert sys)

- Studies show that 70% of actual breach events are NOT detected by the victim-company, but by 3rd parties (and many more go undetected completely).
- False positives: 70%



Patch Management:

- All systems need constant care (patching) to keep bad guys out.
- Complexity of networking environments



Encryption (of private data)

- Problem spans all sizes & sectors.
- Only 2.4% of all breaches had ‘encryption’

How to protect your data?

Ownership of Data

- If you have access and you don't need it, Let IT know
- If you don't need a local copy of data from the system, don't make it.
- Destroy local copies when they are no longer needed

Physical Security

- Laptops
- Backups
- Portable storage

Transmission or Transportation of Data & File sharing

Keep the tools Sharp

What sort of cyber policies are available?

Reputational Injury (B2B / B2C - Disparagement Named Peril)	• Third party is disparaged or has their privacy violated due to the Insured's Cyber Activities • Example: An employee makes a comment in a company e-mail that libels a customer
Conduit Injury (B2B / B2C - System)	• Customers systems are affected by a Cyber-attack launched against the Insured's System • Example: Suit arises from a System security failure that causes a virus to be transmitted from the Insured to a third party's System
Content Injury (B2B / B2C - IP Named Peril)	• Violation of a third party's intellectual property rights via the Insured's System • Example: The Insured displays a logo on its website that violates someone else's trademark.

What sort of cyber policies are available?

Disclosure Injury (B2C - Privacy)

- Individuals are affected by the unauthorized access of their private information held on the Insured's system
- Example: Individual customers' credit card data is stolen from the Insured's System by a hacker
- Coverage enhancements available by Endorsement

Impaired Access Injury (B2B / B2C – Transactional)

- Customers suffer damages because they can't access the Insured's system to conduct a transaction
  - Example: A disgruntled employee Exceeds Authorized Access and Customers can't transact business with the Insured in a timely fashion resulting in the Customer suffering a financial loss

What questions to ask when looking for a cyber policy?

- A stand alone liability policy with optional multiple first party expense coverages with individual sub-limits and retentions
- Intended for Insured's that do transactions over the internet and/or store confidential customer information on their Systems
- Flexibility to allow tailoring for individual clients
- Claims made
- Pay on behalf for liability coverage
- First party expenses paid as incurred

Questions

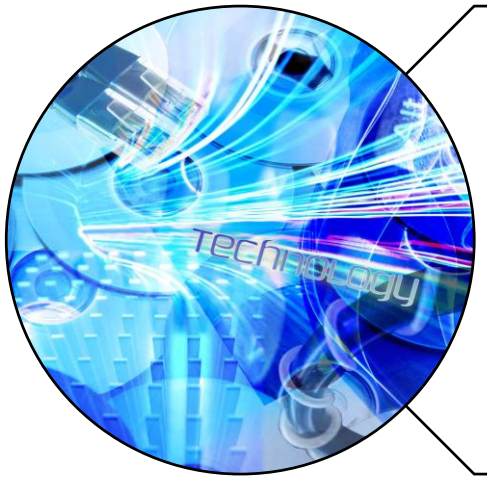
Answers

Agenda for 2014 District Conference

- Electronic Discovery + Litigation Strategy
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics


What is big data?

What is *"Big Data"*



Data whose scale, diversity, and complexity require new architecture, techniques, algorithms, and analytics to manage it and extract value and hidden knowledge from

We use it to refer to refers to the acquisition and analysis of massive collections of information, collections so large that until recently the technology needed to analyze them did not exist. Omer Tene & Jules Polonetsky, *Privacy In The Age Of Big Data: A Time For Big Decision*, 64 Stan. L. Rev. Online 63 (2012).

Big Data Landscape

Vertical Apps

PREDICTIVE POLICING
bloomreach
MYRRIX

Log Data Apps

splunk> loggly sumologic

Ad/Media Apps

rocketfuel collective[i]
bluefin Recorded Future
LuckySort
Media Science TURN DataXu

Business Intelligence

ORACLE | Hyperion
SAP BusinessObjects RJMetrics
Microsoft | Business Intelligence
IBM COGNOS birst
MicroStrategy
Autonomy bime
QlikView
Chart.io GoodData

Analytics and Visualization

tableau Palantir
OPERA metaLayer
METAMARKETS dataspora
TERADATA ASTER centrifuge
SAS TIBCO KARMASPHERE
panopticon Real-Time Visual Data Analysis pentaho
Datameer
platfora ClearStory CIRRO
alteryx visual.ly AYATA

Data As A Service

factual kaggle
knoema beta
GNIP DATASIFT Windows Azure Marketplace INRIX LexisNexis SPACE CURVE LOQATE Everything Location

Analytics Infrastructure

Hortonworks VERTICA An HP Company MAPR TECHNOLOGIES
cloudera INFOBRIGHT PARACCEL
EMC² GREENPLUM
NETEZZA kognitio
DATASTAX EXASOL calpont

Operational Infrastructure

COUCHBASE 10gen The MongoDB company
TERADATA HADAPT
TERRACOTTA VoltDB
MarkLogic INFORMATICA

Infrastructure As A Service

amazon web services
Windows Azure
infochimps
Google BigQuery

Structured Databases

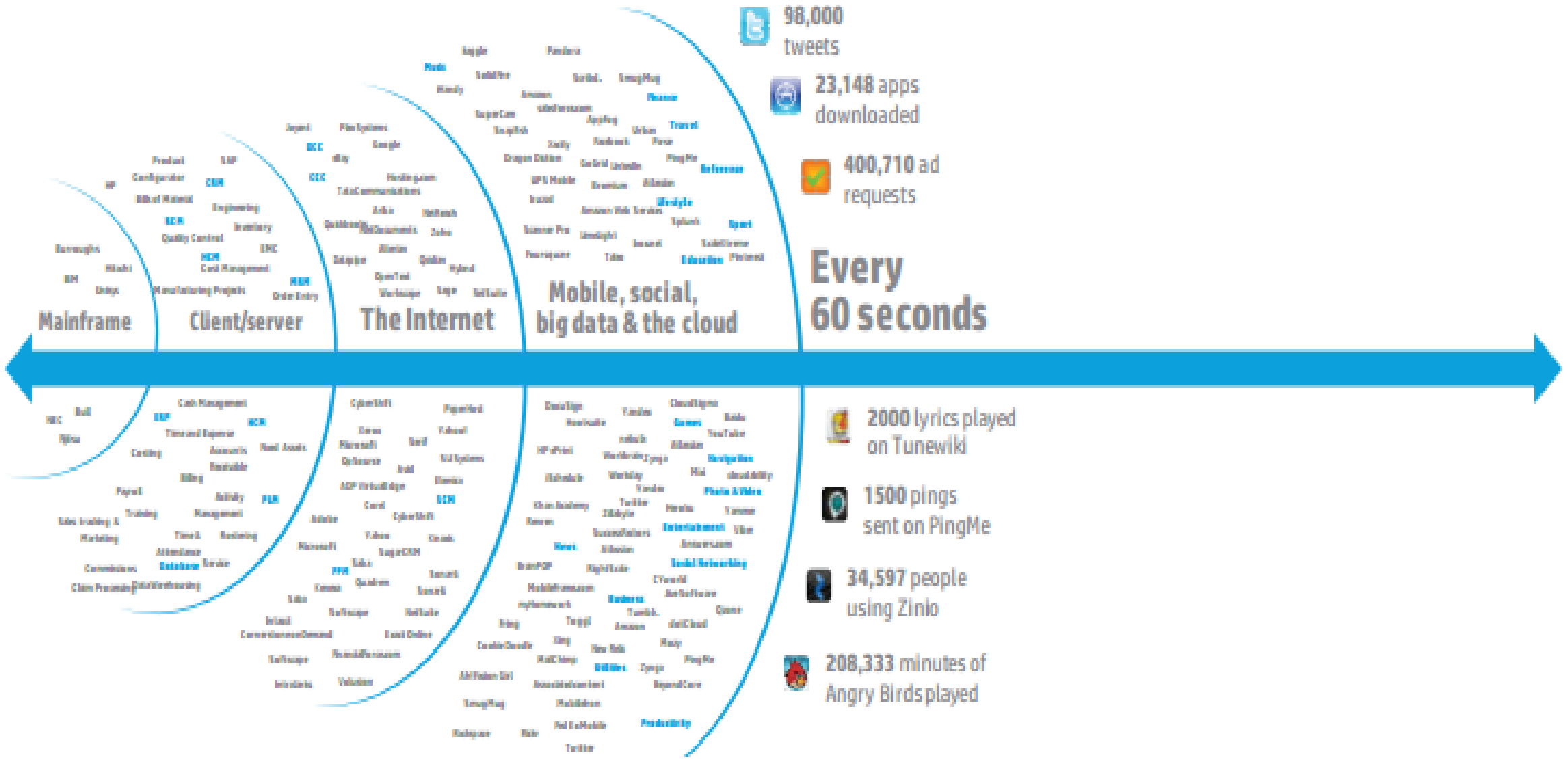
ORACLE MySQL
Microsoft SQL Server PostgreSQL
IBM DB2 SYBASE
memsql

Technologies

hadoop hadoop MapReduce mahout APACHE HBASE Cassandra

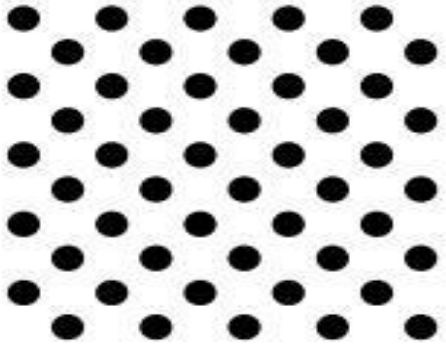
dave@vcdave.com
blogs.forbes.com/davefeinleib

The Data Explosion



Big Data: Volume, Velocity, Variety Veracity

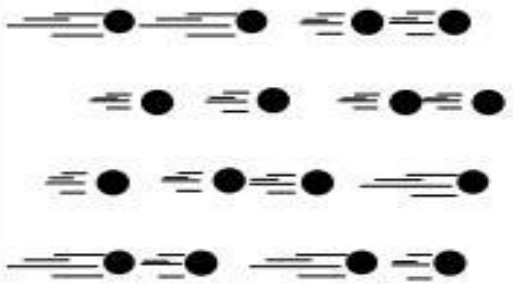
Volume



Data at Rest

Terabytes to exabytes of existing data to process

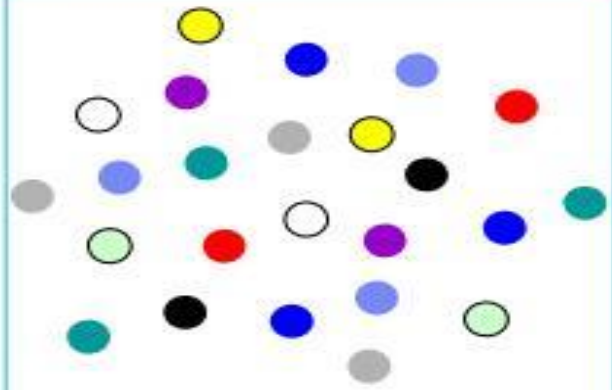
Velocity



Data in Motion

Streaming data, milliseconds to seconds to respond

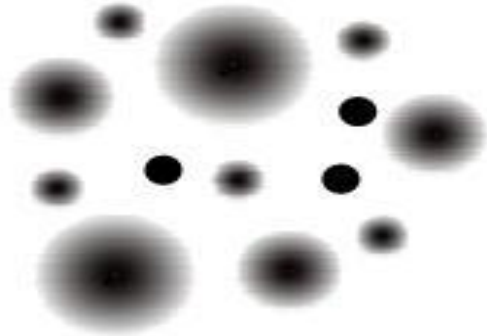
Variety



Data in Many Forms

Structured, unstructured, text, multimedia

Veracity*



Data in Doubt

Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

Why do we care about Big Data?

- **Data is the new oil – we have to learn how to mine it! Qatar – European Commission Report**
- **$ 7 trillion economic value in 7 US sectors alone**
- **$90 B annually in sensitive devices**
- **An insurance firm with 5 terabytes of data on share drives pays $1.5 m per year**
- **New McKinsey 4th factor of production: Land, Labor, Capital, + Data**

Is big data changing litigation?

Yes.

Intellectual property

Antitrust

Class actions

to find relevant needles…

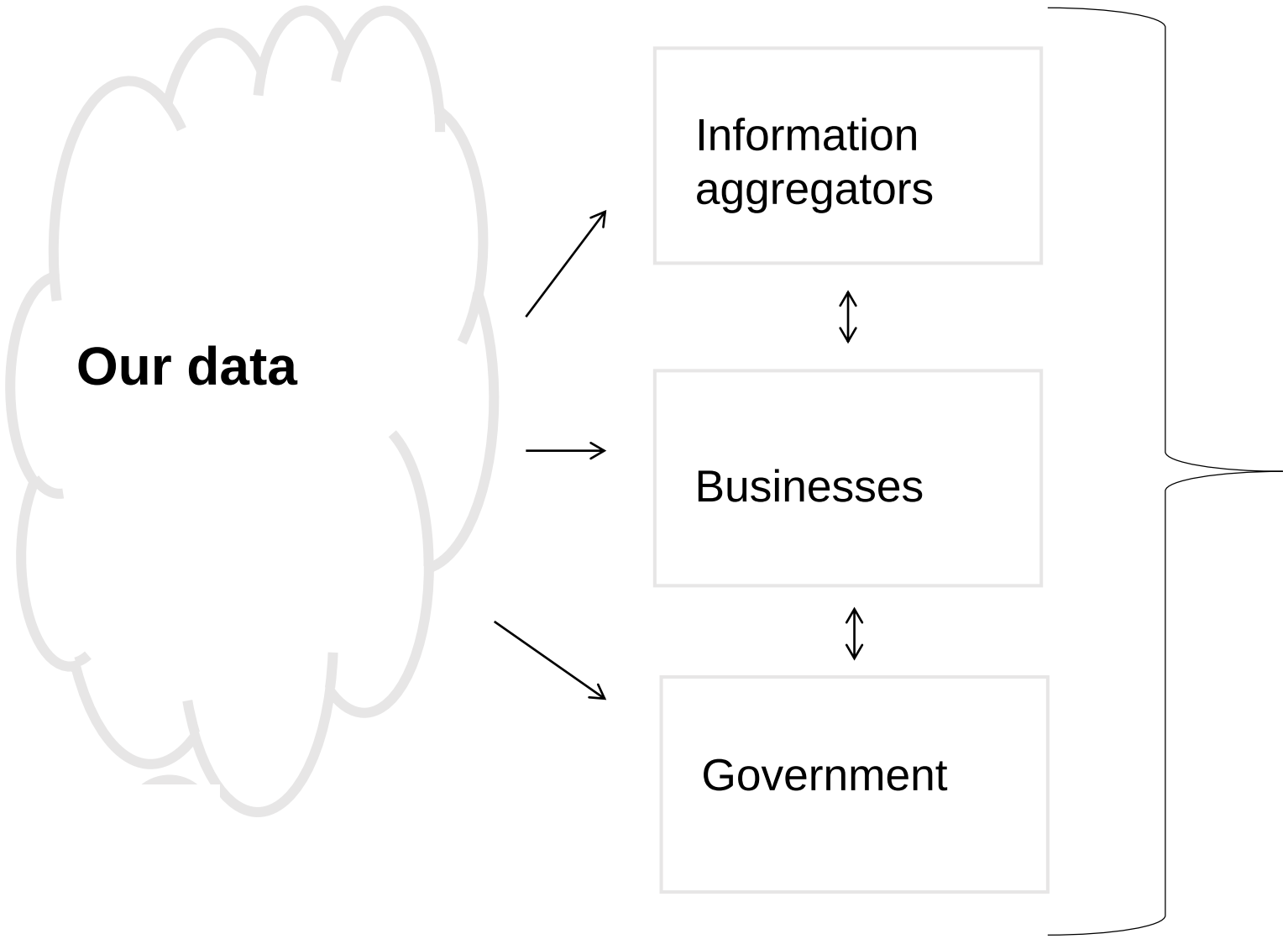
U.S. v. Philip Morris E-mail Winnowing Process

- **20 million email records → 200,000 hits based on keyword terms used (1%) → 100,000 relevant emails → 80,000 produced to opposing party → 20,000 placed on privilege logs**

PROBLEM: only a handful entered as exhibits at trial

A BIGGER PROGLEM: the 1% figure does not scale

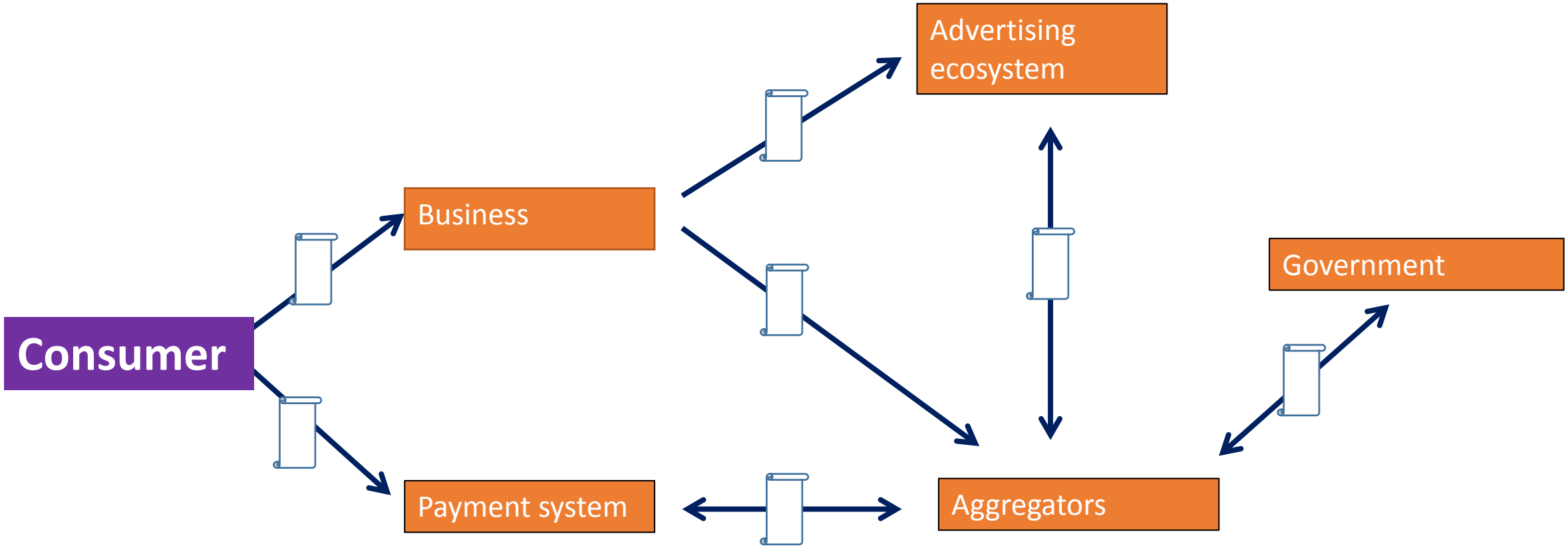
New Privacy Problems in Big Data?



"We can determine where you work, how you spend your time, and with whom, and with 87% certainty where you'll be next Thursday at 5:35 p.m."

What We Have—Contractually Realized Unconstrained Notice and Choice

contractual



How big data is influencing the legal profession?

Class Actions and Story Telling

Class Actions

- Big data in class actions with respect to statistical sampling, which has historically been used to extrapolate about both cause and effect, might no longer be necessary.
- It is possible to easily and quickly review the entire data set and not just a sample, trumps probability-based calculations….will statistical sampling still be allowed?

Story Telling

- Create many opportunities for lawyers to tell a much richer and more real story than they have in the past.

How big data is influencing the legal profession?

Jury Selection

Possibility of having the ability to pull information about prospective jurors from their publicly-available data in real time.

No longer relying on self-reporting.

Google glasses.

And if political candidates can use such data to target their messages, perhaps attorneys will use it to mold their arguments as well.

Questions

Answers

Agenda for 2014 District Conference

- Electronic Discovery + Litigation Strategy
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

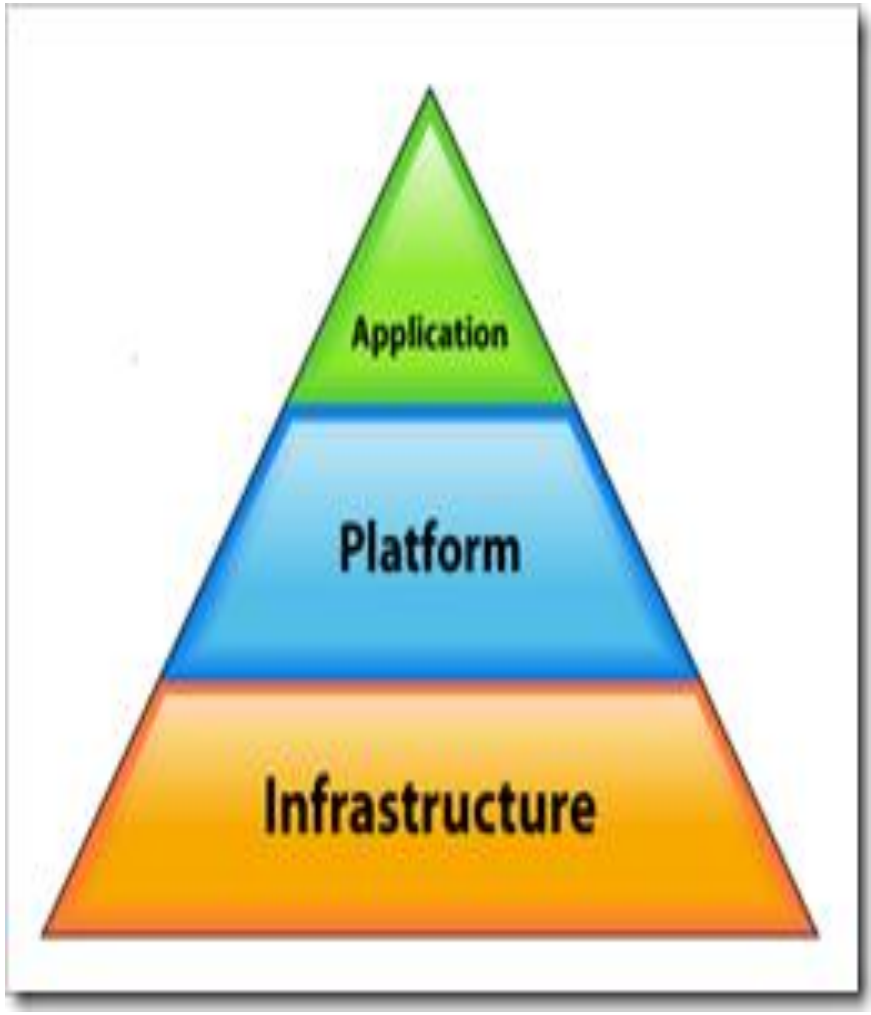
Cloud Computing

Cloud Computing

What is Cloud Computing?

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST definition of Cloud Computing



Cloud Computing

What are the different types of Cloud?

Software as a Service (SaaS)	Hosted a single application	Hotmail, Gmail, Salesforce, Dynamics CRM, Quickbooks Online
	Hosted suite of programs	Microsoft's Office 365 - Exchange Online and SharePoint Online.
		Google Docs
Infrastructure as a Service (IaaS).	Users rent computing power	Either actual hardware or virtualized machines
		Deploy and run your own operating systems and software applications.
Platform as a Service (PaaS).	Users create / run their own applications	
	Cloud provides:	Software development tools
		Underlying infrastructure

Cloud Computing

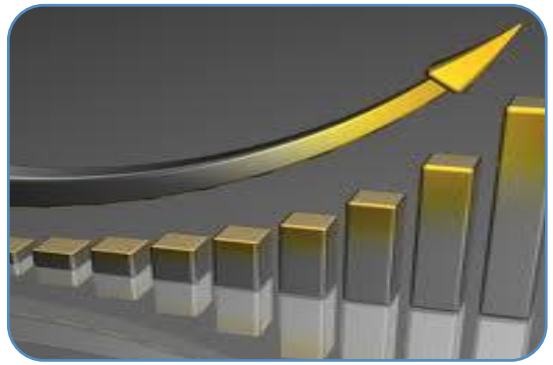
Why go to the Cloud?

Details are abstracted from end-users

No need for expertise in, or control over, the technology infrastructure "in the cloud”

Device and location independence

- Users access systems often using a web browser (e.g., PC, mobile phone)
- Infrastructure is off-site and accessed via the Internet
- Connect from anywhere



Allow business decision to

- Save money
- Focus on their core business

Cloud Computing

What to put in the contract?

Devil is in the details

- What benefits exist
- What risks exist
- What if data is lost or corrupted
- What if service is down
- Who is overseeing authentication and authorization
- What controls to mitigate
- What legal considerations
- Who pays to get data out of cloud?
- Who pays if security breach?
- Who pays for third-party data requests?

Cloud: Cautions and Considerations for Governance

Mobile

$3.6B
spend by 2014

9.6 Billion
connected devices, growing to 22B by 2020

Social

25% productivity
improvement from social enabled processes

96% of GenYers
have joined a social network

Cloud

47%
growth in cloud processes

80% of new commercial enterprise apps are deployed in the cloud

Big Data

$4M
Per year to store and manage a single PB

2.5 Quintillion
bytes of new data generated daily.
Big data and analytics drive insight

Agenda for 2014 District Conference

- Electronic Discovery + Litigation Strategy
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

Questions

Answers


Bring
Your
Own
Mobile
Device
MENU

Mobile Threats to the Corporation and Law Firms

Network
- Unauthorized network access
- Cloud data storage and authentication
- Unencrypted communications

Device
- Rooting
- Jailbreaking
- Lost or stolen device
- Physical manipulation
- SIM card attacks
- Baseband attacks
- DoS attack against the device

User
- Insider data leakage
- Unskilled user / social engineering
- Excessive charges / Fraudulent transactions
- Mobile malware / Spying software / Mobile botnet

Applications
- Poor Authentication and Authorization
- Insecure local data storage
- Client side injection
- Improper session handling
- Security decisions via untrusted input
- Side channel data leakage
- Broken cryptography
- Hard-coded sensitive information
- Malicious code execution
- Privilege escalation
- Insecure user interface
- Bypassing DRM
- Wallet misuse / mCommerce

Services
- Misuse of remote administration
- Unsatisfactorily implemented wipe method

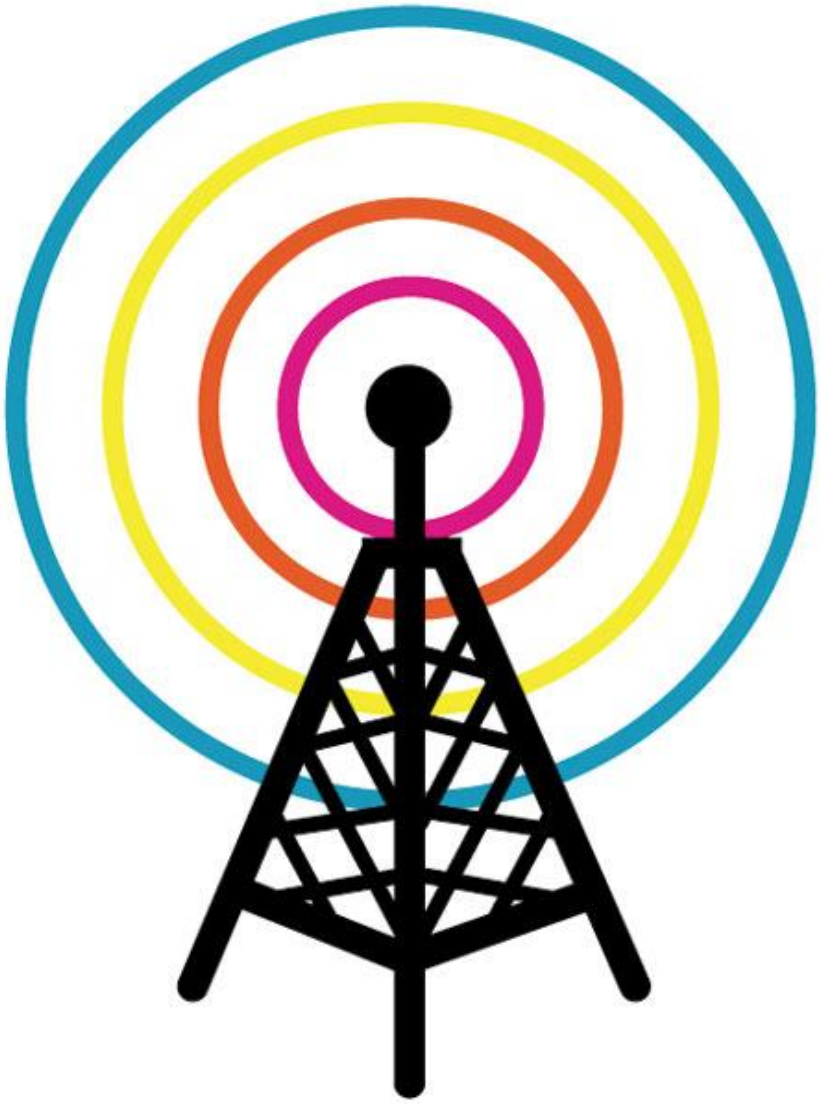
Bring Your Own Device

The mobile "**bring your own device**" (BYOD) era is just beginning and organizations need to react and adapt quickly.

"MOBILE DEVICES" REFERS TO MOBILE PHONES, SMART PHONES, TABLETS AND SPECIALIZED MOBILE COMPUTING DEVICES THAT PRIMARILY CONNECT TO A WIRELESS CARRIER FOR COMMUNICATIONS.

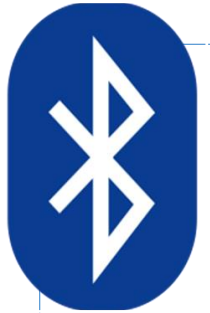
The Evolution of Mobile Phones

- First generation (1G) — analog cellular radio (voice only)
- Second generation (2G) — digital cellular radio (voice and basic data only)
- Third generation (3G) — multimedia cellular radio (audio, data, entertainment, images, video clips, voice, and etc.)
- Beyond 3G/fourth generation/(B3G/4G) – interoperable with other broadband wireless solutions, delivering converged services across different network types, and reducing the costs of delivering data to mobile users utilizing data intensive applications.



Capabilities of Modern Mobile Devices

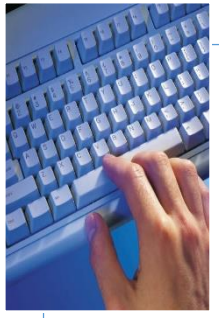
Wi-Fi



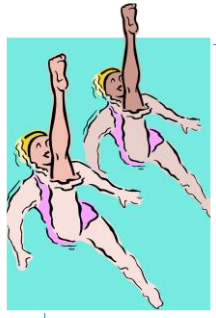
Bluetooth

Multiple Cameras – photography and video capabilities

Information sharing via Near-Field Communication



Check Email



Synchronize across devices

How Mobile Devices Work

Mobile phones and devices can transmit information over cellular signals or wireless signals.

How to Manage BYOD for Employers

Just Cause is Not Good Enough

- Just because you can legally monitor something by law, policy or consent doesn't mean that you should or that it is good management practice.

Give Trust

- If you want a relaxed work environment where employees are trusted and treated as grown-ups, monitoring and discipline over personal phone and computer use will not promote your cause.

Common Sense

- But if you are dealing with sensitive information that requires higher levels of security, then you may need to monitor to protect the business.

Can't have your cake and eat it to.

- But you can't have it both ways – **Just make sure to clearly and conspicuously communicate the level of privacy that can be expected**.

What is the risks to the bench and the bar?

- Who owns the device?
  - BYOD versus CYOD
- Who owns the data?
  - Does it matter, personal versus corporate data?
- No laws specific to BYOD
  - Employers cannot monitor or obtain texts and voicemails on an employee's personal cell phone. A different analysis applies, however, if an employee is spending a lot of time at work loudly talking about personal matters Then, there would be a good argument that it wasn't private and the employee can be disciplined for not working.
  - Sunshine Laws Exception: Texas legislature passed a law in 2013 that makes any state business communications by a state employee, that are conducted on a personally owned device, to be subject to the Public Information Act.

Real World BYOD

Private email accounts that are password protected generally should not be monitored because there is a reasonable expectation of privacy.

Employers Obligations

- Employers should provide notice about the consequences of storing personal content on the same device, under a policy that allows co-mingling of data.
- The employees personal information (including passwords) can be stored during backups
- The personal information can be viewed by monitoring tools, like DLP, and may not be private at all.

Exceptions

- If the employee is conducting any illegal activity on the personal account that must be surrendered to law enforcement or the employer's criminal investigations unit
- If the employee is conducting a personal outside business on company time
- Any other violation of company policy is being conducted on the device

BYOD Legal and Business Benefits

Enabling mobile workers

24/7 work environment

Competitive advantage

Workplace "perk"

- Workers more comfortable and productive

COST SAVINGS

BYOD Risks for the Bench and Clients

Mixing Business and Personal

- Data segregation – the future
- Privacy concerns – Employee, Third parties
- Other "data" – the great American novel (e.g., location tracking, remote wipe)

Workplace injuries

- Repetitive stress and other work related injuries can arise from BYODs.
- Disclaim liability, urge employees to follow vendor recommendations, and check insurance coverages

Information Security

- Extending the corporate security policy to BYOD and enforcing security policies on BYOD
- BYOD security software -- Remote wipe, Tracking, Malware on mobile devices

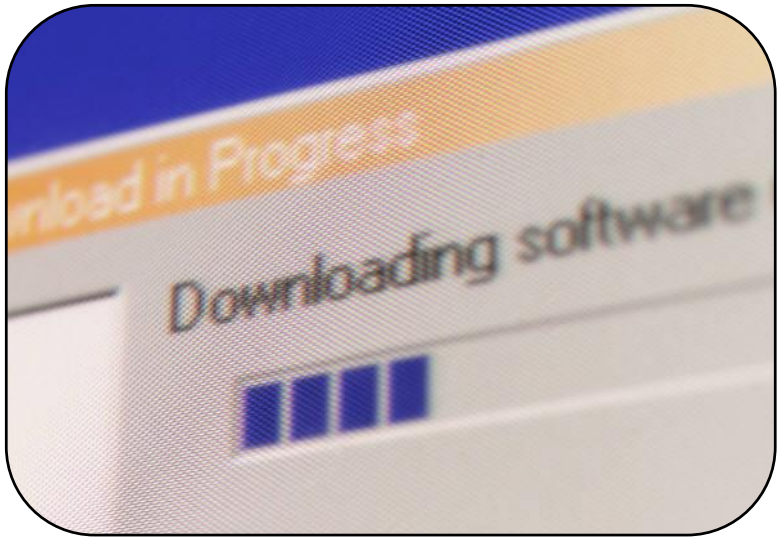
Sharing is Caring

- Friends, family, neighbors, etc. present security implications.
- A risk that cannot be completely controlled and impossible to obtain consent and not clear as to policy coverage
- Company proprietary and confidential information at risk and also privacy issues.

BYOD Risks for the Bench and the Bar

Disposal of Devices

- EOL of BYOD (a/k/a “The eBay threat”) -- Army hardware being sold on streets of Afghanistan or broker-dealer Blackberry on eBay
- Terminated employees likely to be reluctant



Software Licensing

- Company software -- Which applications?, What do the licenses say?
- Employee personal software (e.g., Microsoft Office Home, Picasa, and etc.)
- Get ready for audits

BYOD are fair game in litigation

- Employees must understand -- litigation hold
- Cost of responding to discovery
- Beware at the border -- data and devices can be copied or seized

How to write a BYOD Policy?

- Notice
  - Communicate internally so as to ensure adequate notice
  - Require BYOD employees to agree to policy
- Policy Elements
  - Detail expectations of privacy when on company systems
  - Expressly provide for investigative access to data
  - Detail security requirements:
    - Allow “jail broken” or “rooted” devices?
    - Require security software or PIN locks?
  - Explain what happens when:
    - Device is lost or stolen
    - Employee leaves the company
    - Any protective software is not installed or uninstalled

Ten BYOD Tips.

1. Get employee consent if you going to allow mobile devices in workplace and familiarize yourself with the types of devices already used by employees. Aim to support the mostly common devices first.
2. Purchase anti-virus and malware protection for mobile devices.
3. Balance risk and benefit for more advanced BYOD solutions.
4. Encrypt the data stored on the mobile device.
5. Make sure that you are able to remotely wipe mobile devices if necessary.
6. Don’t punish employees for reporting loss personal mobile device.
7. Establish Mobile Device Use Policies and segregate Data.
8. Know your legal limits of securing and monitoring personal devices used to transmit corporate information.
9. Educating employees about how to handle mobile devices is critical.
10. Don’t let your executives get a free pass.

Agenda for 2014 District Conference

- Electronic Discovery + Litigation Strategy
- Amended FRCP (Dec. 2015)
- Key Word Search
- Cyber Security
- Big Data
- Cloud Computing
- BYOD
- Digital Forensics

Digital Forensics

What is digital forensics?

Digital Forensics is the preservation and analysis of electronic data.

WHY DO WE HAVE TO DEAL WITH DIGITAL FORENSIC ANALYSIS?

In cases where information is hidden, erased, or otherwise altered, digital forensic analysis is necessary to draw further conclusions about the available evidence.

What can computer data tell you?

Business and personal correspondence

Identification and recovery of files that have been deleted from a computer

Usage patterns of a computer, or the sequence of events, can be ascertained

Identification of date and time related information, including document provenance

The person performing an action on a computer

Password protected files

Consider how you use your computer

Types of information on computers

- Active files
  - User generated files (Word, Excel, PowerPoint, Adobe etc)
  - Document templates
  - System generated temporary files
  - E-mail messages
  - Internet activity
  - Internal log files
  - Instant messages
  - Faxes and voicemail
- Deleted versions of active files
- Fragments of previously deleted files

What are Benefits of Forensic Expert?

- Understanding if the evidence you have in hand is worth analysing.
- Acquiring potentially relevant data sources
- Determining if ESI is relevant
- Recovering deleted information
- Accessing password protected documents
- Restoring data from backup tapes
- Providing expert evidence and testimony
- Advising counsel on drafting, responding, and requesting information about your client's electronic documents

Potential situations

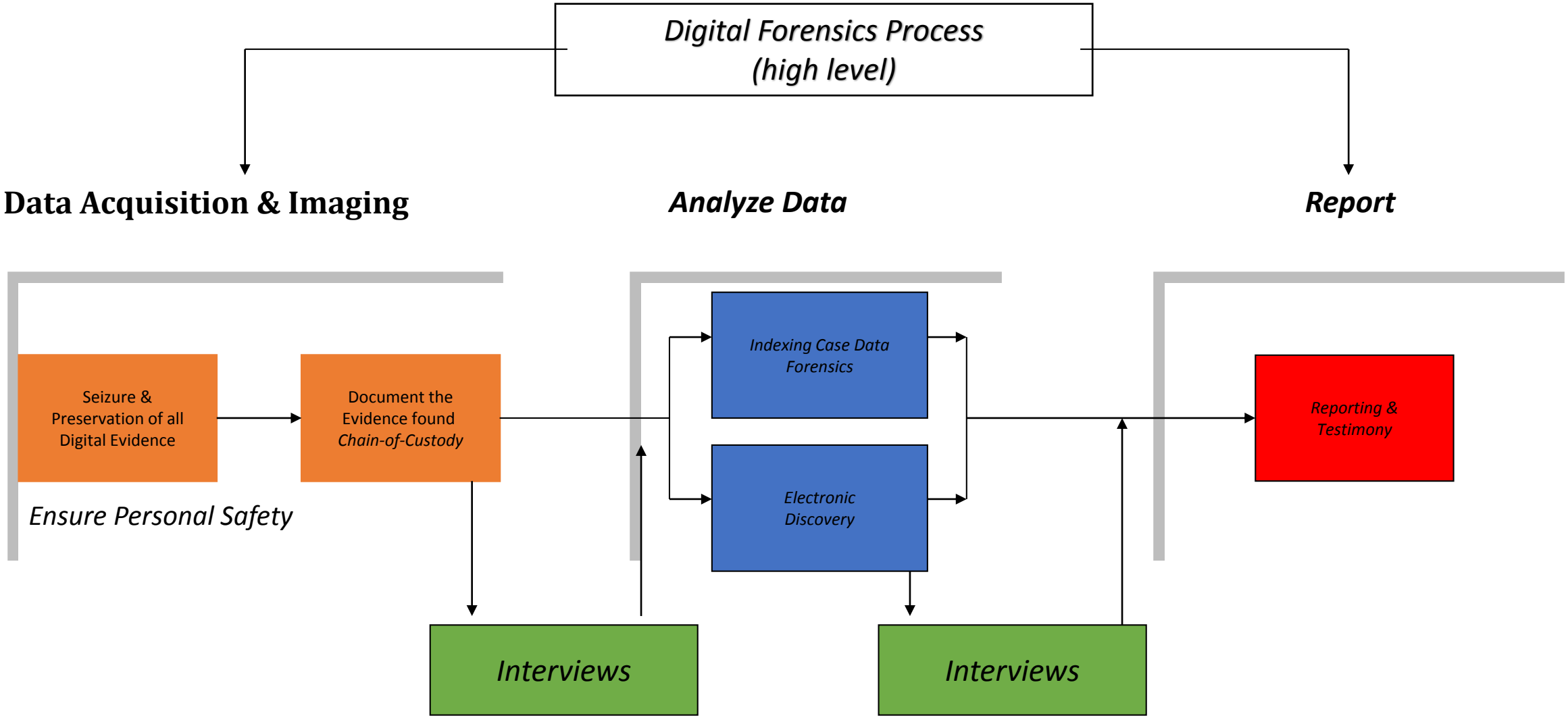
- Financial investigations
- Insider trading by employees
- FCPA investigation by subsidiary actors
- Intellectual property theft by employees, competitors, or State actors
- Execution of Court orders
- Employees forming competing businesses
- Fraud and bad employee investigations
- Identification and secure removal of data from computer systems – often done in acquisitions.

What goes into a forensic investigation?

Digital Forensics in Traditional Forensic Context

Primary substantive data	Secondary data.	Investigator
The gun and the drugs	**Fingerprints.**	**Robbery/Homicide**
The Hack	Hard-drive containing primary data, data trails, and time stamps.	Forensic/Malware Examiner

Details of a Forensic Investigation



Gaining access to the data

Basic Forensic Concepts

After image files have been generated, backup tapes located and provided, and files collected the data must be accessed

Active, and deleted, files can be extracted out of image copies

Backup tapes typically require an appropriate environment to be constructed to enable the data to be restored

Backup tapes typically require about a half day per backup tape to restore the data

Once the data has been restored and extracted a suitable culling and review strategy is required

Practical considerations for data collection

Relevant data may be resident on many different sources:

- Personal computers
- Network servers (file and e-mail servers)
- Backup tapes
- Removable media (CD-ROMs, “thumb drives” etc.)

Different methodologies can be implemented for data collection dependant upon the type of matter, importance of custodian, and level of acceptable business disruption

- Generating image copies
- Provision of backup tapes
- Legal / IT team supervision of file collection
- Requesting of files from individuals

Generating an image copy

If a particular computer is thought to contain data vital to a matter an image copy should be generated

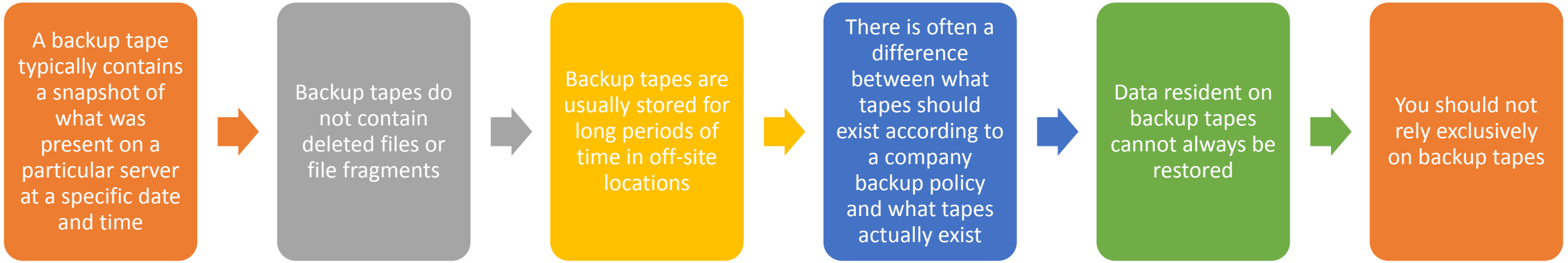
The “image copy” of the hard disk in the computer should be generated by a forensic computing professional

The image copy contains all of the data resident on the computer including active and deleted files

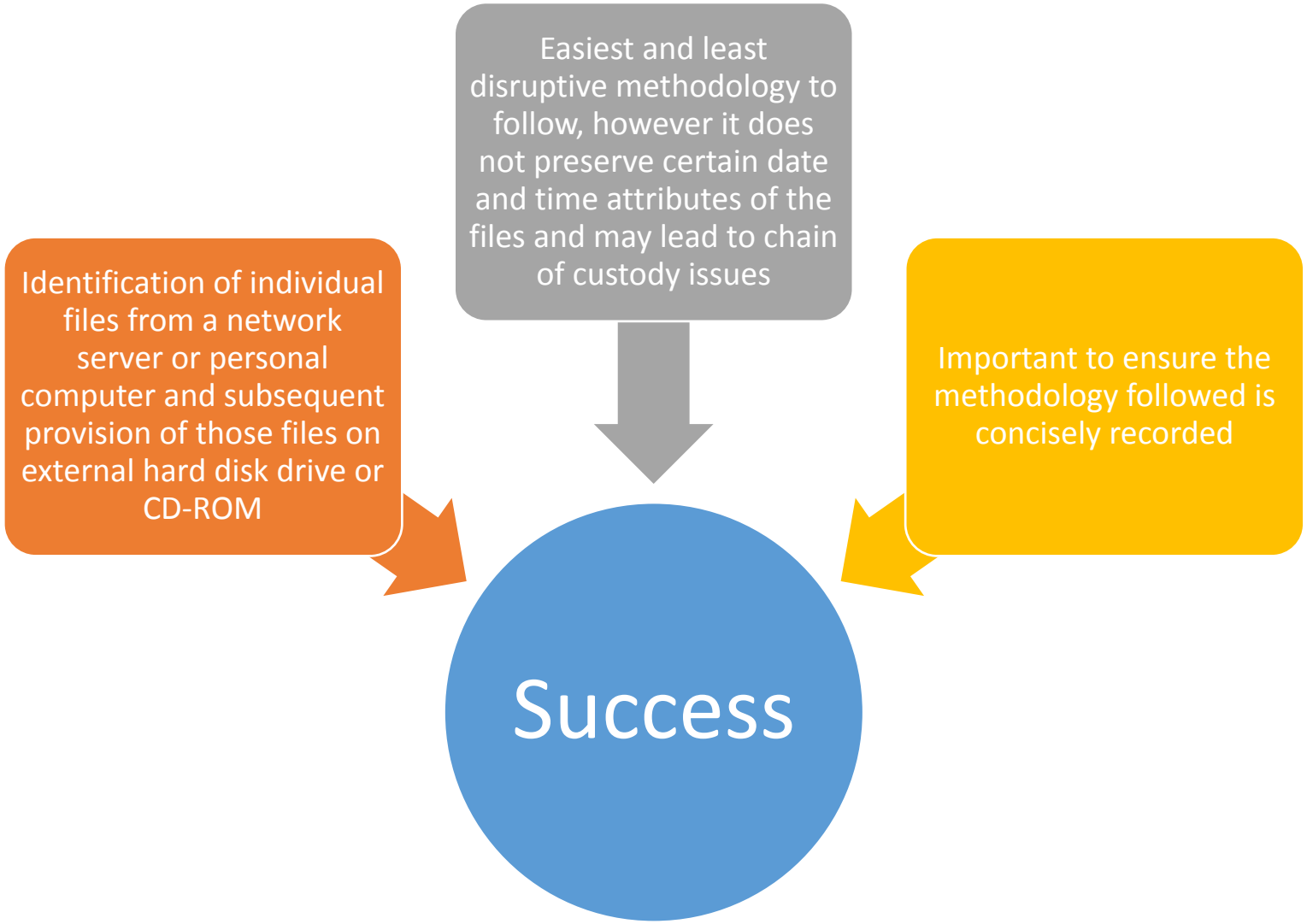
Specialist technology enables the image copy to be generated from an “average” business computer in approximately two hours

The image copy can either be generated on or off-site

Practical considerations for backup tapes



Practical considerations for file collection



Applications of Computer Forensics

Employee internet abuse

Unauthorized disclosure of corporate information l

Industrial espionage

Damage assessment

Criminal fraud and deception cases

- FCPA

What should be in a forensic report?

Structure of a Digital Forensic Report

Brief summary of information
Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
Evidence Item #1 (For example A's work computer) -- Summary of evidence found on Employee A's work computer.
Analysis of relevant portions of Employee A's work computer -- Email history, Internet search history, USB registry analysis
Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
Recommendations and next steps for counsel to continue or cease investigation based on the findings in the report

Devil is in the details

Sufficient Details to Replicate Findings.

Document.	Should document with sufficient detail the steps undertaken by the examiner so that an independent third–party could replicate the conclusions.
Forensic Images.	Forensic images should be available for copying by a third-party. Digital forensic report is less dependable when the forensic images are not available to replicate the findings because of the inability to assess its accuracy or the reliability of its methodology.
Reproducible.	Reports with conclusions that are not reproducible using copies of the forensic images and similar analysis should be granted little credence, and only reviewed in extraordinary circumstances.

Questions

Answers

LAW & FORENSICS

Managing Partner
Daniel Garrie
Law & Forensics

(855) 529 – 2466

www.lawandforensics.com

daniel@lawandforensics.com

www.linkedin.com/danielgarrie