DIGITAL FORENSICS

Forensic (Legal) Studies

Work Overview

- Interview legal luminaries (local forensics)
- Readings and other sources (encyclopedia and existing international and local proceedings, law dictionary)
- Berkman Cyber Law, Harvard Internet and Society
- United Nations on Digital and Multimedia Forensics
- Internet Society Policy on Security and Forensics, if any
- [Foreign, US] Supreme Court, Department of Commerce, NIST-SP, FBI (existing subject laws and relevant laws or links to other existing laws)
- [PH] Supreme Court, Department of Justice, National Bureau of Investigation Digital Forensic (references to existing laws, existing subject and relevant laws)

PARTS

I. Overview of digital forensics and evidence
II. Courtroom and trial preparations
III. Computer crimes legislation, enforcement law and legal considerations (majority with foreign jurisprudence)
  - Legal definitions
  - Legal pursuits
  - Associated disciplines / subdivisions
IV. Forms of evidence
V. Cybercrimes and expert witness
VI. Standards governing expert witness and scientific evidence
VII. Budapest convention on cybercrime
VIII. Philippines laws, jurisprudence and relevant practices
IX. Case studies
X. Philippines cases

OVERVIEW OF DF AND EVIDENCE

Digital Forensic

- Branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime
- Expanded to cover investigation of all devices capable of storing digital data
- Applications are variety and the most common is to support or refute a hypothesis before criminal or civil (as part of e-discovery process) courts.
- Has roots in the personal computing revolution of the late 1970s and ‘80s
- The discipline evolved in a haphazard manner during the 1990s
- The early 21st century has emerged national policies

Digital Forensic continuation

- Can be used to attribute evidence
  - Specific suspects
  - Confirm alibis
  - Statements
  - Determine intent
  - Identify source (e.g. copyright cases)
  - Authenticate documents

What Is Digital Evidence?

- It is an information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

What Is Digital Evidence? continuation

- Is latent, like fingerprints or DNA evidence
- Crosses jurisdictional borders quickly and easily
- Is easily altered, damaged, or destroyed
- Can be time sensitive

What Is Digital Evidence? continuation

LEGAL AUTHORITY EXISTS TO COLLECT EVIDENCE

COURTROOM AND TRIAL PREPARATION

Courtroom & Trial Preparation

- Begins at the outset of investigation
- The presentation of digital evidence requires familiarity with
  - Specialized
  - Evolving, and
  - Sometimes complex technology
- The need for technical competence runs throughout the case

Courtroom & Trial Preparation continuation

- It is essential that investigators and prosecutors
  - Acquire a basic working knowledge of the technical aspects of digital evidence in general
  - Master the specific technical details of the case at hand
- Preliminary considerations that the prosecutor needs to take into account when reviewing the scope of the investigation to date
- Effective pre-trial communication among prosecutors, investigators and examiners
- Evidentiary issues e.g. authentication, hearsay, et al

Courtroom & Trial Preparation: Preliminary Considerations

- Cases involving digital evidence should be developed by a team that consists of the prosecutor, lead investigator, and the examiner
  - Such cases often present special procedural and substantive issues
- One of prosecutor's first task is to review the scope of the investigation

Courtroom & Trial Preparation: Preliminary Considerations cont'n

- One of prosecutor's first task is to review the scope of the investigation. Several key issues include
  - Is the digital evidence associated with a ***"high-technology" crime***?
  - Is digital evidence nevertheless an important aspect of the case? Or is digital evidence simply involved in the investigation or presentation of the case? (For example, a prosecutor may use a computer simulation or animation to illustrate an expert's testimony.)

Courtroom & Trial Preparation: Preliminary Considerations cont'n

- Identifying and explaining the source and nature of the digital evidence in the case
  - Do the storage devices contain evidence of the crime or are they themselves evidence or instrumentalities of the crime?
  - What hardware, software, operating systems, and system configurations were used by the target of the investigation or by the victim?
  - Was the evidence found on a stand-alone personal computer or a network?

Courtroom & Trial Preparation: Preliminary Considerations cont'n

- Considering whether additional sources of digital evidence should be investigated (e.g., backup files, log files)
- Considering all appropriate charges (e.g., does a child pornography possession case also involve dissemination charges?)

Courtroom & Trial Preparation: Pretrial Communication

- The prosecutor, investigator, and examiner should meet well in advance of trial to plan the presentation of the case
  - **Discuss any points for which clarification, further analysis, or additional investigation may be needed.**
    - Ensure familiarity with the specific technological aspects of the case.
    - Review the experience and qualifications of the investigator and examiner.

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Review the scope and limitations of the evidence.
- Read the reports prepared by the investigator and examiner before the meeting and use the meeting to clarify any points of uncertainty

– **Conduct a pretrial meeting with the investigator and examiner to clarify the legal theory of the case, the elements of the crimes charged, and any anticipated defenses**
– **Review with the investigator and examiner the likely scope and direction of direct and cross-examination**

Courtroom & Trial Preparation: Pretrial Communication cont'n

- **Distinguish the types of digital evidence.**
  - Three broad categories of digital evidence raise issues that are especially important to address in a pretrial meeting
    - Background evidence,
    - Substantive evidence, and
    - Illustrative evidence
  - Each category of evidence also requires clarifying whether a witness will testify as an expert

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Background evidence on technological issues
  - Will the examiner be asked to provide general background testimony as well as testimony concerning the results of his or her analysis?
  - Are there general technical issues that are not in dispute? If so, can they be presented at the outset on a stipulated basis apart from the case-specific testimony?
  - Does the use of metaphors or analogies to illustrate the technological issues present any legal complications? Using metaphors may have unintended consequences (e.g., referring to computers or computer files as "containers" may have Fourth Amendment implications).
  - Should a stipulated glossary of undisputed technical terms be provided to the trier of fact?

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Substantive evidence. Tactical considerations:
  - Should e-mail messages and other digital evidence be presented in hard copy or on screen?
  - Will the jury be able to review hard copies of digital evidence in the jury room?
  - Should all relevant files or only specific examples be offered? If all are to be offered, should all of them or only specific examples be discussed? How should sample files (e.g., files in a child pornography case) be selected?
  - Digital evidence may include voluminous records for which summaries may be appropriate.

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Substantive evidence. Technical considerations:
  - Addressing technical glitches during trial (e.g., arrange for technical support, provide backup or hard copies)
  - Preparing the courtroom for presentation of digital evidence
    - Ensure the computers are functional
    - Check that adequate and appropriate equipment is available and in working order, and that wiring and functional outlets are in place
    - Notify court security that special equipment will be in the courtroom
    - Notify the court reporter if audio will be presented
    - Consider the placement of monitors and lighting issues

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Substantive evidence. Technical considerations:
  - Presenting the evidence
    - Have clean copies of exhibits
    - Ensure adequate setup time
    - Ensure that standby mode, startup screen, sound (if applicable), and screen savers are deactivated

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Substantive evidence. Technical considerations:
  - Presenting the evidence Remember where presentation ended at the last break (i.e., cueing)
    - Create an adequate court record by fully describing referenced exhibits. Consider asking the court to allow nontraditional means of recording the presentation of evidence (e.g., videotape of computer presentations, printouts of screen captures, CD-ROMs)
    - Provide jury notebooks or exhibit books
    - Consider whether to request jury note taking

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Illustrative evidence
  - In addition to the foregoing sets of tactical and technical issues, illustrative evidence may present additional considerations, such as:
    - Which presentation medium or combination of media will be most persuasive.
    - Whether to present animation in a fixed form that cannot be altered to accommodate changed assumptions or in a form that can be modified.
    - Whether such evidence will need to be disclosed pretrial.

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Pretrial rulings consideration
  - Because digital evidence may be unfamiliar to the court and may seem complex, consider resolving admissibility (e.g., of expert testimony) and presentation issues by pretrial motion

Courtroom & Trial Preparation: Pretrial Communication cont'n

- Pretrial rulings consideration
  - Goals
    - Avoids addressing those issues for the first time at trial before the jury
    - Educates the court about technology-related issues
    - Secures admission of evidence at trial
    - Identifies potentially objectionable evidence

Courtroom & Trial Preparation: Evidentiary Considerations

- (THIS PARTICULAR NOTE MAY APPLY IN ACCORDANCE WITH THE U.S. FEDERAL RULES OF EVIDENCE (FRE) ONLY)
- Evidentiary considerations may be affected by the nature and source of the digital evidence. This section discusses the following:
  - Defining evidentiary terms
  - Preexisting substantive evidence stored on a computer
  - Preexisting substantive evidence generated by a computer
  - Substantive and illustrative computer-generated evidence prepared for trial
  - Expert testimony

Courtroom & Trial Preparation: Defining Evidentiary Terms

- Judicial discretion
- Relevance (does the evidence help?)
  - "Relevant evidence" is broadly defined to mean "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence" (FRE 401).

Courtroom & Trial Preparation: Defining Evidentiary Terms cont'n

- Of the various relevance-based objections, two are of particular concerns
  - Prejudice
  - Other actions

- Authentication (is it what you say it is?)
- Hearsay (the preference for live testimony)

Courtroom & Trial Preparation: Defining Evidentiary Terms cont'n

- Hearsay (the preference for live testimony)
  - Is it hearsay?
  - If it is hearsay is it nevertheless admissible under one of the exceptions?

Courtroom & Trial Preparation: Preexisting SE Computer Stored

- Distinguishing substantive from illustrative evidence and computer-stored from computer-generated evidence
  - Substantive vs illustrative
  - Computer stored vs computer generated

Courtroom & Trial Preparation: Authentication Computer-Stored

- Substantive evidence
- Common ways to authenticate email
  - The chain of custody following the route of the message, coupled with testimony that the alleged sender had primary access to the computer on which the message originated
  - The content of the e-mail refers to matters of which the writer would have been aware
  - The recipient used the reply function to respond to the e-mail; the reply may include the sender's original message
  - After receiving the e-mail, the sender takes action consistent with its content

Courtroom & Trial Preparation: Hearsay and Computer-Stored

- The computer equipment (hardware and software) on which the record was stored is recognized as standard in the field or reliable
- The data were entered in the regular course of business at or reasonably near the time of the occurrence of the event recorded
- The sources on which the record was based, as well as the method and time of preparation, indicate the record is trustworthy and its admission is justified

Courtroom & Trial Preparation: Hearsay and Computer Stored cont'n

- This foundation may be established through the testimony of the custodian of the record or by a person who is familiar with the methods by which it was prepared, even if that person does not have personal knowledge of the underlying facts contained in the record and is not a computer expert familiar with the technical aspects of the software or hardware. In support of establishing trustworthiness, the prosecution might show:
  - Company reliance on the data
  - Protection of the accuracy of data entry
  - Prevention of loss or alteration of the data while in storage
  - Provision for integrity of data output

Courtroom & Trial Preparation: Printouts Computer-Stored

- Requirement of the original, or best evidence, rule
  - The so-called “best evidence” rule generally requires a party seeking to prove the contents of a writing, recording, or photograph to introduce the original writing, recording, or photograph unless an exception applies (FRE 1002).

Courtroom & Trial Preparation: Printouts Computer-Stored cont'n

- Summaries
  - Under FRE 1006, if the contents of voluminous writings, recordings, or photographs cannot be conveniently examined in court, a party may present them in the form of a chart, summary, or calculation—subject to limitations such as making the originals or duplicates available to the other party for inspection or copying

Courtroom & Trial Preparation: Preexisting SE Computer Generated

- Authentication of preexisting substantive evidence generated by a computer
- Hearsay and preexisting substantive evidence generated by a computer

Courtroom & Trial Preparation: S&I Computer Generated Evidence

- Types of evidence
- Evidentiary issues
  - Relevance
  - Manner of interrogation
  - Authentication and other foundation issues
  - Hearsay

Courtroom & Trial Preparation: Expert Opinion Testimony

- Using opinions of an expert witness calls for a threefold approach:
  - Identify the issues that will require an expert opinion
  - Identify a qualified expert
  - Ensure that the qualified expert will use an admissible method

Courtroom & Trial Preparation: Expert Opinion Testimony cont'n

- The admissibility of expert opinion testimony may be challenged prior to trial. The prosecutor and the expert should prepare to meet the pretrial challenge as carefully as preparing for the trial itself.

COMPUTER CRIMES LEGISLATION (FOREIGN JURISPRUDENCE)

Computer Crimes Legislation

- Were dealt with using existing laws prior to the 1980s
- Were first recognized in the 1978 Florida Computer Crimes Act (in the U.S.)
  - Included legislation against the unauthorized modification or deletion of data on a computer system
- 1983, Canada was the first country to pass legislation
- 1986, U.S. Federal Computer Fraud and Abuse Act (included in the Comprehensive Crime Control Act fo 1984), amended a number of times in 1989,1994, 1996, in 2001 by USA Patriot Act, 2002 and in 2008 by Identity Theft Enforcement and Restitution Act (ITERA)
- 1989, Australian amendments to their crimes acts
- 1990, British Computer Abuse Act
- 2012, Cybercrime Prevention Act, on TRO (as of 8 July 2013)

Digital Forensic Investigation Law Enforcement

- Regulation of Investigatory Powers Act, UK, ability of UK law enforcement to conduct digital forensics investigations is legislated by it
  - An Act about the interception of communications, the acquisition and disclosure of data relating communications, the carrying out of surveillance, the use of covert human intelligence sources
  - To take account of technological change such as the growth of the Internet and strong encryption

Digital Forensic Legal Considerations

- Covered by national and international legislation
- For civil investigations, in particular, laws may restrict the abilities of analysts to undertake examinations
  - Restrictions against network monitoring, or reading of personal communications often exist
- During criminal investigation, national laws restrict how much information can be seized
  - Examples, see next slide

Digital Forensic Legal Considerations continuation

- PACE Act, UK, governs the seizure of evidence by law enforcement
  - Other laws that may affect forensic investigators, also in UK, is the 1990 Computer Misuse Act, which legislates against unauthorized access to computer material, particularly for civil investigators, who have more limitations than law enforcement

U.K. on 802.11 Capable Computers Legal Req't Examples

- European spectrum on operating wireless LAN
- Particularly Austria, Belgium, France and Switzerland
- Channels include
  - 52, 56, 60, 64 (Indoor, Austria at 5250-5350MHz)
  - 104, 108, 116…140 (Indoor/Outdoor, Austria, Belgium, France, Switzerland at 5470-5725MHz)

U.K. on 802.11 Capable Computers Legal Req't Examples cont'n

- The 5GHz turbo mode feature is not allowed for operation in any European Community country
- Such device must not be operated in ad-hoc mode using channels in 5GHz bands in the European Community
- Such device, if use, must be used with access points that have employed and activated a radar detection feature required for European Community operation in the 5GHz bands

Digital Forensic Legal Considerations continuation

- Electronic Communications Privacy Act, US, places limitations on the ability of law enforcement or civil investigators to intercept and access evidence
  - It makes a distinction between stored communication e.g. email archives, and transmitted communications such as VOIP
    - The latter being considered more of a privacy invasion, is harder to obtain a warrant for
  - It affects the ability of companies to investigate the computers and communications of their employees, an aspect that is still under debate as to the extent to which a company can perform such monitoring
  - Article 5 of the European Convention on Human Rights asserts similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with external countries

IOCE

- The International Organization on Computer Evidence is one agency that works to establish compatible international standards for the seizure of evidence

General Laws, Provisions and Definitions

- Criminal code (penal code) contain offences which are recognised in the jurisdiction, penalties which might be imposed for these offences and some general provisions (such as definitions and prohibitions on retroactive prosecution)

General Laws, Provisions and Definitions continuation

- Criminal law is the body of law that relates to crime. It regulates social conduct and proscribes threatening, harming, or otherwise endangering the health, safety, and moral welfare of people. It includes the **punishment** of people who violate these laws

General Laws, Provisions and Definitions continuation

- Civil law means non-criminal law. The law relating to civil wrongs and quasi-contracts is part of the civil law. Civil law can, like criminal law, be divided into substantive law and procedural law. Civil law is the branch of law **dealing with disputes** between individuals or organizations, in which compensation may be awarded to the victim.

General Laws, Provisions and Definitions continuation

- Common law legal system is a system of law characterized by **case law** which is law developed by judges through decisions of courts and similar tribunals

General Laws, Provisions and Definitions continuation

- Statute is a formal written enactment of a legislative authority that governs a state, city, or country. Typically, statutes command or prohibit something, or declare policy. Statutes are sometimes referred to as legislation or "black letter law. A source of law, considered **primary authority**.

General Laws, Provisions and Definitions continuation

- Primary authority is a term used in legal research to refer to statements of law that are binding upon the courts, government, and individuals. Primary authority is usually in the form of a document that establishes the law, and if no document exists, is a legal opinion of a court. The search for applicable primary authority is the most important part of the process of legal research.

General Laws, Provisions and Definitions continuation

- Examples of primary authority include the verbatim texts of:
  - Constitutions;
  - Basic laws;
  - Statutes (whether codified or uncodified);
  - Treaties and certain other international law materials;
  - Municipal charters and ordinances;
  - Court opinions;
  - Rules of court procedure;
  - Rules of evidence;
  - Rules governing the conduct of lawyers;
  - Administrative regulations;
  - Executive orders.

General Laws, Provisions and Definitions continuation

- Secondary authority is an authority purporting to explain the meaning or applicability of the actual verbatim texts of primary authorities (such as constitutions, statutes, case law, administrative regulations, executive orders, treaties, or similar legal instruments).

Digital Forensic Legal Pursuits

- Recognized as one of the first examples was Clifford Stoll's investigation of Markus Hess
  - Co-operation was gaining from law enforcement, was a challenge due to the relatively new nature of the crime
  - Investigation has been described in "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" and "Stalking the Wily Hacker", the former chronicled in an episode of WGBH's NOVA "The KGB, the Computer and Me"

Associated Disciplines / Subdivisions

- Computer forensic
- Forensic data analysis
- Database forensics
- Network and Internet (cyber) forensics
- Forensic video
- Forensic audio

Jurisprudence

The science of the law. By science here, is understood that connection of truths which is founded on principles either evident in themselves, or capable of demonstration; a collection of truths of the same kind, arranged in methodical order. In a more confined sense, jurisprudence is the practical science of giving a wise interpretation to the laws and making a just application of them to all cases as they arise. In this sense, it is the habit of judging the same questions in the same manner, and by this course of judgments forming precedents.

Litigation

A science that describes analysis or data developed or produced expressly for use in a trial versus those produced in the course of independent research. This distinction was made by the US 9th Circuit Court of Appeals when evaluating the admissibility of experts.

FORMS OF EVIDENCE

Evidence

- Broadly construed, is anything presented in support of an assertion.
- All the means by which any alleged matter of fact whose truth is investigated at judicial trial is established or disproved
- Stand as proof of
- Basis of belief or disbelief, knowledge on which to based belief
- In law, the production and presentation of evidence depends first on establishing on whom the burden of proof lies.

Rules of Evidence

- Code of evidence law governing the admission of facts by which parties (in the US federal court system) may prove their cases, both civil and criminal
- Rules which govern the admissibility of evidence into court

Burden of Proof

- The obligation of a party in an argument or dispute to provide sufficient evidence to shift the other party's or a third party's belief from their initial position.
- Two principle considerations
  - On whom does the burden of proof rest?
  - To what degree of certitude must the assertion be supported?
- Other legal standards of proof include
  - Reasonable suspicion, probable cause, prima facie evidence, credible evidence, substantial evidence and clear and convincing evidence

Forms of Evidence

- Demonstrative evidence
- Real evidence
- Testimony
- Scientific
- Eyewitness identification
- Genetic
- Lies
- Documentary
- Digital
- Exculpatory

Demonstrative Evidence

- In the form of a representation of an object
- Opposed to, real, testimony or other forms of evidence used at trial
- Useful in assisting finder of fact in establishing context among the facts presented in a case.
- To be admissible, it must be "fairly and accurately" represent the real object at the relevant time
- Must be "relevant" just like any other kind of evidence
- Examples of demonstrative evidence
  - Photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations and models

Real Evidence

- Also called material evidence or physical evidence
- Any "material object", introduced in a trial, intended to prove a fact in issue based on its demonstrable physical characteristics
- Can conceivably include all or part of any "object"
- Is usually reported upon by an expert witness with appropriate qualifications to give an opinion
- Examples include
  - Written contract, defective part or defective product, murder weapon, gloves use by an alleged murderer, trace evidence—fingerprints, glove prints and firearm residue, biological evidence—DNA left by the attacker on victim's body, weapon used, pieces of carpet spattered with blood or casts of footprints or tire prints found at the scene of the crime.

Real Evidence continuation

- Admission of real evidence requires
  - Authentication, demonstration of relevance, and a showing that the object is in the same or substantially the same condition
- Authentication can be through witness statements or by circumstantial evidence called the chain of custody
- Evidence that conveys in a different form the same information that would be conveyed by a piece of physical evidence is not itself physical evidence
  - Example: A diagram comparing a defective part to one that was properly made is documentary evidence—only the actual part, or a replica of the actual part, would be physical evidence

Testimony Evidence

- A solemn attestation as to the truth of a matter or make the declaration of fact
- "Testimony" and "testify" have a root in the Latin *testis,* referring to the notion of a third person, disinterested witness
- It may be oral or written and is made by oath or affirmation under penalty of perjury

Testimony Evidence continuation

- When a witness is asked a question, the opposing attorney can raise an objection, mentioning one the standard reasons, including:
  - Argumentative or inflammatory
  - Asked or answered
  - Best evidence rule
  - Calls for speculation
  - Calls of conclusion
  - Compound question or narrative
  - Hearsay
  - Irrelevant, immaterial, incompetent
  - Lack of foundation
  - Leading question
  - Privilege
  - Vague
  - Ultimate issue terstimony
  - Non-responsive

Testimony Evidence continuation

- The statement made by a witness under oath or affirmation. Vide Bill to perpetuate testimony.

Scientific Evidence

- Serves to either support or counter a scientific theory or hypothesis
- Expected to be empirical evidence and in accordance with scientific method
- In law, it is derived through forensic evidence i.e. digital forensics

Documentary Evidence

- Any evidence introduced at a trial in the form of documents
- While it is most widely understood to mean writings on paper i.e. invoice, contract or will, the term actually include any media by which information can be preserved including photographs, tape recordings, films and printed emails

Documentary Evidence continuation

- Example
  - If a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary
- Subject to specific forms of
  - Authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author
  - Best evidence rule, requires that the original document be produced unless there is a good reason not to do so

Digital Evidence

- Called electronic evidence
- Any probative information stored or transmitted in digital form that a party to a court case may use at trial
- Examples include
  - Email, Digital, Photographs, ATM transaction logs, Word processing / spreadsheet, Instant message histories, Internet browser, Files in accounting programs, Databases, Volatile data, Backups, printouts, GPS tracks, Electronic door locks, Digital video or audio

Digital Evidence continuation

- Courts in the U.S. sometimes treated digital evidence differently for purposes of the following:
  - Authentication, hearsay, best evidence rule and privilege
- Federal Rules of Civil Procedures (U.S.) enacted requiring preservation of electronically stored evidence, and when attacked for its authenticity, courts reject such argument unless there is proof of tampering
- Discovery Plan (sample form from U.S. District Court of New Hampshire) http://www.nhd.uscourts.gov/ru/Form-SampleDiscoveryPlan.asp?print=true

Digital Evidence continuation

- Best evidence rule (deprecated)
  - A common law rule of evidence which can be traced back at least as far as the 18th century
  - Check out Blackstone's Criminal Practice (is not all but defunct) and Lord Denning MR (do not confine to the best evidence. The goodness or badness of it goes only to weight, and not admissibility)

Relevance of Evidence

- Burden of proof
- Laying a foundation
- Public policy exclusions
- Spoliation
- Character
- Habit
- Similar fact

Authentication of Evidence

- Chain of custody
- Judicial notice
- Best evidence rule
- Self authenticating document
- Ancient document
- Hague evidence convention

Hague Evidence Convention

- Called the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters
  - Multilateral treaty which was drafted under the auspices of the Hague Conference on Private International Law

Legal Challenges

- Evidence (digital media for evidentiary purposes)
  - Search, seizure, (reconstruction?) and presentation
- Existence of laws (e-commerce, related laws outside of electronic context)
  - Legal coverage
  - Legal processes
  - Legal research
- Criminal procedure and law
  - Criminal (and civil?) investigation and litigation
    - Depositions and counter-arguments
    - Testimonies
- Technical / expert support to legal practitioners on DF cases

Common Attack on Digital Evidence

- Digital media can be easily altered
- Early court decisions required that authentication called
  - For a more comprehensive foundation (US v Scholle, 553 F.2d 1109 (8th Circuit, 1976))
- As courts became more familiar with digital documents, they back away from the higher standard and have since held that
  - Computer data compilations should be treated as any other record (US v Vela, 673 F.2d 86, 90 (5th Cir. 1982))
  - The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness (US v Bonallo, 858 F.2d 1427 – 1988 – CA 9th)

American Law Reports

- A resouce used by American lawyers to find a variety of sources relating to specific legal rules, doctrines and principles.
- Lists a number of ways to establish the 'more comprehensive foundation' required by *Scholle*, which still remain a good practice include
  - The reliability of the computer equipment
  - The manner in which the basic data was initially entered
  - The measures taken to insure the accuracy of the data as entered
  - The method of storing the data and the precautions taken to prevent its loss
  - The reliability of the computer programs used to process the data
  - The measures taken to verify the accuracy of the program

CYBERCRIMES AND EXPERT WITNESS

Cybercrimes Involving

- White collar
- Technology expert
- Employee
- Spies or opportunistic hackers

Cybercrimes Include

- Corruption
- Embezzlement / fraud
- Theft
- Ponzi
- Money laundering
- Election fraud

White Collar Investigation and Litigation

- 15 Minutes in the Life of Joe Ford, 27 September 2007, AICPA National Conference on Fraud and Litigation
  - Internet as conduit for crime as it is commerce
  - Reviewed terabytes electronic media including email
  - Forensic accountants and blueprint for investigation
  - Convictions numerous
  - $1.6Bn settlement

Technology Expert Conviction and Appeal

- Hacking of, or a neglect within, AT&T servers specifically collecting customers's email address belonging to iPad 3G users
  - Andrew 'Weev' Auernheimer, convicted on violation to Computer Fraud and Abuse Act (CFAA)
- Case study on Weev's conviction and appeal

Bank Employee Conviction

- Supervisor in the electronic marketing department
- Duties include overseeing customer transactions especially returned mail items as undeliverable such as
  - Debit cards
  - PIN
- $50k unauthorized transactions related to undeliverable debit cards and PINs

Money Laundering

The process of concealing the source of large amounts of money that have been gained through illegitimate means. Money evidently gained through crime is "dirty" money, and money that has been "laundered" to appear as if it came from a legitimate source is "clean" money. Money can be laundered by many methods, which vary in complexity and sophistication.

Money Laundering continuation

- Is a financial thought crime
- Intergovernmental body
  - Financial Action Task Force on Money Laundering (FATF) – especially setup to combat money laundering
- Governmental authority
  - AMLA under BSP, IC and SEC supervision

Money Laundering Notable Cases

- Bank of Credit and Commerce International: Unknown amount, estimated in billions, of criminal proceeds, including drug trafficking money, laundered during the mid-1980s.
- Bank of New York: US$7 billion of Russian capital flight laundered through accounts controlled by bank executives, late 1990s
- In December 2012, HSBC: paid a record $1.9 Billion fines for money-laundering hundreds of millions of dollars for drug traffickers, terrorists and sanctioned governments such as Iran. The money-laundering occurred throughout the 2000s.

Money Laundering Notable Cases continuation

- In May 2013, Liberty Reserve was seized by United States federal authorities for laundering $6 billion.
- Nauru: US$70 billion of Russian capital flight laundered through unregulated Nauru offshore shell banks, late 1990s
- Sani Abacha: US$2–5 billion of government assets laundered through banks in the UK, Luxembourg, Jersey (Channel Islands), and Switzerland, by the president of Nigeria.
- Standard Chartered: paid $330 million in fines for money-laundering hundreds of billions of dollars for Iran. The money-laundering took place in the 2000s and occurred for "nearly a decade to hide 60,000 transactions worth $250 billion".

Election Fraud

- Nowadays, many government have become a vociferous users of computerization especially during election periods.
  - Philippines, started nationwide, fully automated election system in 2010
    - There have been claims, none have/had been proven and ended to be a talk shop everywhere
  - Russia, which WSJ have gone through extraordinary lengths to prove a foreign election fraudulent
    - WSJ used computers/written program to download 2.957 web pages on Russia's Central Election Commission

Crimes Through Which Computers Were Crucial

- Multimillion (if not billion) dollar companies
- Financial market traders
- Securities company executives

Crime Perpetrated Within Company

- Enron was an American energy, commodities, and services company based in Houston, Texas
- Caused the de facto dissolution of Arthur Andersen, one of the 5 largest audit and accountancy partnership in the world
- Scandal
  - Went bankrupt based on revelation in October 2001
  - CFO misled board of directors and audit committee on high risk accounting practices, pressured Andersen to ignore the issues
  - Many executives indicted and later sentenced to prison
  - Found guilty in US District Court
  - Overturned by US Supreme court
  - Lost many customers and closed
  - Lost billions in pensions and stock prices

Enron Scandal

- Went bankrupt based on revelation in October 2001
- CFO misled board of directors and audit committee on high risk accounting practices, pressured Andersen to ignore the issues
- Many executives indicted and later sentenced to prison
- Found guilty in US District Court
- Overturned by US Supreme court
- Lost many customers and closed
- Lost billions in pensions and stock prices

Enron Scandal continuation

- Caused to enact the **Sarbanes-Oxley Act** on 30 July 2002, expanded the accuracy of financial reporting for public companies and increased penalties for destroying, altering, or fabricating records in federal investigations or for attempting to defraud shareholders.
- **The Act is nearly 'a mirror image of Enron**: the company's perceived corporate governance failings are matched virtually point for point in the principal provisions of the Act'

Enron Scandal continuation

- Andersen would shred several tons of relevant documents and delete nearly 30,000 **emails** and **computers files**, causing accusations of a cover up

Enron Corpus

- Large database of over 600,000 emails generated by 158 employees
- Acquired by Federal Energy Regulatory Commission during its investigation after the company's collapse
- A copy was bought by Andrew McCallum, computer scientist at University of Massachusetts Amherst

Enron Corpus Copy

- Released to researchers
- Provided a trove of data
- Used for studies
  - Social networking
  - Computer analysis of language
- The corpus is unique
  - 1 of the only publicly available mass collections of real emails easily available for study

Enron Corpus Copy continuation

- Benefitted the community of researchers and the public alike with the following:
  - EDRM (which guidance was discussed in 1st module) published a revised version 2 of the copy which provided
    - Over 1.7 million of messages, available in Amazon S3 for easy access
    - Data Set Cleansed by PII by Nuix and EDRM

Enron Data Set Cleansed (Enron Corpus)

- Nuix case study
  - "Investigating the prevalence of unsecured
    - financial,
    - Health, and
    - personally identifiable information in corporate data"

The Source Data Comprises

- 1.3 million emails messages and attachments from former Enron staff
- 168 MS Outlook .PST files
- Almost 40GB of data

STANDARDS GOVERNING EXPERT WITNESS AND AND SCIENTIFIC EVIDENCE

Forensic (Legal) Studies

EDRM Data Set Project

- Provides
  - Industry standard
  - Reference data sets of electronically stored information (ESI)
  - Software files that can be used to test various aspects of e-discovery software and services

EDRM Data Set Project: Organizations Cannot Ignore Risks

- PHF data are a serious business risk
- Many organizations do not take steps to address these issues based on two assumptions
  - We don't have to worry unless our systems are hacked
  - The information is there, but no one can find it
- Both assumptions are false

Nuix Case Study: Removing PII

- Personally identifiable information
- EDRM Enron data set is an industry-standard collection of email data that the legal profession has used for many years for electronic discovery training and testing
- The result of the study ‘present food for thought’ about the prevalence of private data in all corporate data sets and the serious business risks it represents

Nuix Case Study: Removing PII continuation

- Established recommendation on
  - Thick blanket of privacy legislations in Western countries, and that
  - Organizations must take extreme care to protect any PII and PIH they store relating to employees or customers

Nuix Case Study: Removing PII continuation

- Regulations and standards that made up due with the dataset includes
  - European Commission's proposed General Data Protection Regulation will impose fines of up to 2% of a company's annual global turnover for failure to protect consumer's PII
  - US Department of Commerce guide to protecting PII for federal government agencies details a long list of
    - Operational safeguards
    - Privacy specific safeguards
    - Security controls

Nuix Case Study: Removing PII continuation

- Organizations that accept credit card payments must also comply with
  - Payment Card Industry Data Security Standards, at present it is PCI DSS v2
    - Imposed by the credit card companies primarily AMEX, Visa, Mastercard and so on
    - Failure to comply with can result in that organization losing its ability to process credit card payments

Nuix Case Study
Readings & Analysis

- Understanding the methodology used
- Identifying the results of the investigation
- How many items have been identified especially about PII
- The type of PII identified
- Is the situation better or worse today?
- The information that can be stored and taken outside the ‘company premises’

Traders Inflicted and Investigated of Crimes

- John Rusnak
  - At Allfirst Financial (US)
  - Turned over the following
    - Bank accounts
    - Spending records
    - **Harddrive** (laptop), used at home for some of his trading

Executives / Accomplice Computer Programmers Convicted

- Bernard Madoff
  - American stockbroker, investment advisor, financier and later white collar criminal
  - Committed the largest financial fraud in US history
- Jerome O'Hara and George Perez
  - Madoff's computer programmers, constructed 'house of cards' to defraud investors for decades
  - The **computer codes** and **random algorithm** they developed served to deceive investors and regulator and concealed Madoff's crimes

Bernard Madoff

- Orchestrated the largest, longest and widespread Ponzi scheme in history.
- Plead guilty to
  - Money laundering
  - Securities fraud
  - Mail fraud
  - Wire fraud
  - Investor advisor fraud
  - Filing false statements
  - Perjury and theft from an employee benefit plan
- Sentenced to 150 years in prison
- Prosecutors estimated at the sentencing hearing that losses in Madoff's accounts since 1996 approach $13 billion

O'Hara & Perez

- Madoff fraud would not have been possible, without their help
- Used their **special computer skills to create sophisticated, credible and entirely phony trading records** that were critical to the success of Madoff's scheme for so many years
- Wrote programs that generated thousands of pages of fake trade blotters, stock records and other bogus documents to substantiate nonexistent trading

O'Hara & Perez And Their Prosecutors Findings

- The computer programs allows Frank DiPascalli (Madoff lieutenant) and other employees to alter records
- Deleted about **218 of 225 special programs** from a computer known as **House 17**
  - Used to process money management account data
  - Cashed out hundreds of thousands of dollars from their personal accounts at Madoff's firm before confronting him and refusing to generate more bogus records
- Essentially the only 2 **programmers** who worked on House 17
- **Concealed the fraud from regulators** and others

Mail and Wire Fraud Madoff-related Coverage Issues

- Computer fraud insuring agreement covers "**direct loss of, or direct loss from damage to, money, securities and other property directly caused by computer fraud**."

Madoff-related Coverage Issues continuation

- Employed "**electronic funds transfers and computers to accomplish his frauds**"
  - **Computer generates** statements and found them to match market results
  - **Computer prepares** manipulated statements for security- and date-specific pricing data
  - **Computer depicts** numerous false purchases and sales of securities at actual market prices

U.S. Wire Fraud Expanded

- 3 elements to mail and wire fraud
  - Intent
  - Scheme or artifice to defraud or the obtaining of property by fraud, and
  - Mail or wire communication
- Wire fraud has been expanded by Congress to include foreign wire communications or interstate connections via an **email server** or telephone switch or radio communication

Mail and Wire Fraud: Title 18 of the United States Code § 1343

- Title 18 of the US Code is the criminal and penal code of the federal government of the United States. It deals with federal crimes and criminal procedure
- It has been a federal crime in the US since 1872
- Chapter 43 is specifically for Mail Fraud and under it is Section 1343 applies to fraud by wire, radio, television and the expanded provisions which include specifically "email server"

Mail and Wire Fraud: Title 18 of the United States Code § 1343 cont'd

- Fine under this title or imprisonment not more than 20 years or both
- If violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years or both
- The blockbuster fraudulent schemes here: https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/FraudSchemes.aspx

Admissibility of Expert Witness

- Daubert standard (US)
  - A party may raise a Daubert motion, which is a special case of motion *in limine* raised before or during trial to exclude the presentation of unqualified evidence to the jury
  - Articulation of Daubert standard relate to the Daubert trilogy including
    - Daubert v. Merrell Dow Pharmaceuticals
    - General Electric Co. v. Joiner
    - Kumho Tire Co. v. Carmichael

Standards Governing Expert Witness and Scientific Evidence

- United States
  - Daubert standard
  - Frye standard or general acceptance test
  - Federal Rules of Evidence 702
- Philippines (general law i.e. electronic-related)
  - Revised Penal Code
  - E-Commerce Act
  - Data Privacy Act
  - Cybercrime Prevention Act

Daubert Standard

- It is the law in federal court and over half of the states
- Florida recently passed a bill to adopt said standard which took effect on 1 July 2013
- In *Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 570 (1993),* the Supreme Court held that the Federal Rules of Evidence superseded Frye as the standard for admissibility of expert evidence in federal courts

Frye Standard or General Acceptance Test

- The court in Frye held that expert testimony must be based on scientific methods that are sufficiently established and accepted
- States still following the standard: California, Illinois, Kansas, Maryland, Minnesota, New Jersey, New York, Pennsylvania, Washington (as of 24 September 2013)

Frye Standard or General Acceptance Test continuation

- Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while the courts will go a long way in admitting experimental testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made **must be sufficiently established to have gained general acceptance** in the particular field in which it belongs

Court Guidelines Admitting Scientific Expert Testimony

- Judge is gatekeeper
- Relevance and reliability
- Scientific knowledge = scientific method/methodology
- Factors relevant

Judge is Gatekeeper

- Under Rule 702 of the Federal Rules of Evidence, the task of "gatekeeping" or assuring that scientific expert testimony truly proceeds from "scientific knowledge", rests on the trial judge

Judge is Gatekeeper / Rule 702, Testimony by Experts

- A witness qualified as an expert by knowledge, skill, experience, training, or education, my testify thereto in the form of an opinion or otherwise, if

(1) the scientific, technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue

(2) the testimony is based upon sufficient facts or data,

(3) the testimony is the product of reliable principles and methods, and

(4) the expert has reliably applied the principles and methods to the facts of the case. (As amended 17 April, effective 1 December 2000)

Relevance and Reliability

- Requires the trial judge to ensure that the expert's testimony is "relevant to the task at hand" and that it rests "on a reliable foundation"

Scientific Knowledge = Scientific Method

- A conclusion will qualify as scientific knowledge if the proponent can demonstrate that it is the product of sound "scientific method"

Factors Relevant

- The Court (US) defined "scientific methodology" as the process of formulating hypotheses and then conducting experiments to prove or falsify the hypothesis and provided a nondispositive, nonexclusive, "flexible" set of "general observations" (i.e. not a test) that it considered relevant for establishing the validity of scientific testimony

Factors Relevant continuation

- Empirical testing, whether the theory or technique is falsifiable, refutable, and/or testable
- Whether it has been subjected to peer review and publication
- The known or potential error rate
- The existence and maintenance of standards and controls concerning its operation
- The degree to which the theory and technique is generally accepted by a relevant scientific community

Daubert Trilogy: Daubert v. Merrell Dow Pharmaceuticals

- Held in 1993 that Rule 702 of the Federal Rules of Evidence did not incorporate the Frye "general acceptance" test as a basis for assessing the admissibility of scientific expert testimony, but that the rule incorporated a flexible reliability standard instead

Daubert Trilogy: General Electric Co. v Joiner

- Held that a district court judge may exclude expert testimony when there are gaps between the evidence relied on by an expert and his conclusion, and that an abuse-of-discretion standard of review is the proper standard for appellate courts to use in reviewing a trial court's decision of whether it should admit expert testimony

Daubert Trilogy: Kumho Tire Co. v. Carmichael

- Held in 1999 that the judge's gatekeeping function identified in Daubert applies to all expert testimony, including that which is non-scientific

Daubert Standard: Appellate-level Opinions

- Case: Daubert v Merrell Dow Pharmaceuticals, Inc #90-55397
  - Argued and submitted March 22, 1994
  - Decided January 4, 1995

BUDAPEST CONVENTION ON ELECTRONIC EVIDENCE

Forensic (Legal) Studies

Budapest Convention on Cybercrime

- Common criminal policy aimed at the protection of society
- Adoption of appropriate legislation and fostering international co-operation
- Protect legit interest in the use and development of information technologies
- Deter action directed against confidentiality, integrity and availability of computing systems
- Facilitate detection, investigation and prosecution at both the domestic and international levels
- Provide arrangement for fast and reliable international co-operation

Budapest Convention on Cybercrime continuation

- Ensure proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the following (especially)
  - 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms
  - 1966 UN International Covenant on Civil and Political Rights
  - 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - 1989 UN Convention on the Right of the Child
  - 1999 International Labour Organization Worst Forms of Child Labour Convention
- Reaffirm the right of everyone to hold opinions without interference
- Right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and the right concerning the respect for privacy
- Enable the collection of evidence in electronic form of a criminal offense

Budapest Convention on Cybercrime continuation

- Title 1, Offences Against CIA
  - Article 2, illegal access
  - Article 3, illegal interception
  - Article 4, Data interference
  - Article 5, System interference
  - Article 6, Misuse of devices

Budapest Convention on Cybercrime continuation

- Title 2, computer-related offences
  - Article 7, computer-related forgery
  - Article 8, computer-related fraud
- Title 3, content-related offences
  - Article 9, offences related to child pornography

Budapest Convention on Cybercrime continuation

- Title 4, offences related to infringements of copyright and related rights
  - Article 10, offences related to infringements of copyright and related rights
- Title 5, ancillary liability and sanctions
  - Article 11, attempt and aiding or abetting
  - Article 12, corporate liability
  - Article 13, sanctions and measures

PHILIPPINE LAWS AND JURISPRUDENCE

Forensic (Legal) Studies

Philippine Laws (the big picture)

- Electronic Commerce 2000 (R.A. 8792)
  - Rules on Electronic Evidence
- Data Privacy Act 2012 (R.A. 10173)
- Cybercrime Prevention Act 2013 (R.A. 10175)

Philippine Laws (the big picture) continuation

- Philippine criminal laws
  - The body of laws defining crimes and defining the penalties thereof
    - Revised Penal Code
      - Took effect 31 January 1932
      - 2 parts
        - » Book 1: Provides the general provisions on the application of the law and the general principles of the criminal law
        - » Book 2: Defines the specific crimes and the penalties imposable for each crime
    - Special Penal Laws

Special Penal Laws

- Forms part of the Philippine criminal laws
- Penalizing acts such as illegal possession and trafficking of dangerous
  - Drugs
  - Money laundering
  - Illegal possession of firearms

Malum's

- Criminal offenses can be broken down into two general categories
  - *malum in se* and
  - *malum prohibitum*.

Malum's Distinction

- *Malum in se* offense is "naturally evil as adjudged by the sense of a civilized community,"
- *Malum prohibitum* offense is wrong only because a statute makes it so. *State v. Horton*, 139 N.C. 588, 51 S.E. 945, 946 (1905).

Mala In Se Examples

- Murder
- Rape
- Theft

Mala Prohibita Examples

- Building or modifying a house without a license
- Copyright infringement
- Gambling
- Illegal drug use
- Operating a business without a license
- Prohibition of alcohol
- Prostitution
- Surrogacy for profit
- Weapon possession

E-Commerce Act, R.A. 8792, Chapter 1

- Section 2. Declaration of policy. Ensures:
  - Network security
  - Connectivity and neutrality of technology for the national benefit
  - Need to marshall
  - Organize and deploy national information infrastructures comprising both telecommunications network and strategic information services and their interconnection to the global information networks
  - Appropriation of legal, financial, diplomatic and technical framework, systems and facilities

E-Commerce Act, R.A. 8792, Chapter 1 continuation

- Section 3. Objective. Aims to facilitate:
  - Domestic and international dealings
  - Transactions, arrangements, agreements, contracts
  - Storage of information through utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and realibility of electronic documents
  - Promote universal use of electronic transaction in the government and general public

E-Commerce Act, R.A. 8792, Chapter 1 continuation

- Section 4. Sphere of application. Applications:
  - Any kind of data message and electronic document used in the context of commercial and non-commercial activities in domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information

E-Commerce Act, R.A. 8792, Chapter 2

- Section 6. Legal recognition of data messages
- Section 7. Legal recognition of electronic documents
  - Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and be authenticated so as to be usable for subsequent reference

E-Commerce Act, R.A. 8792, Chapter 2 continuation

  - For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.
- Section 8. Legal recognition of electronic signatures. The electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure
- Section 9. Presumption relating to electronic signature

E-Commerce Act, R.A. 8792, Chapter 2 continuation

- Section 10. Original documents.
  - Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if
    - The integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence aliunde or otherwise

E-Commerce Act, R.A. 8792, Chapter 2 continuation

  - Where it is required that information be present, that the information is capable of being displayed to the person to whom it is to be presented

- The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display

E-Commerce Act, R.A. 8792, Chapter 2 continuation

- The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all relevant circumstances
- Section 11. Authentication of electronic data messages and electronic documents.
  - Such documents including electronic signatures shall be authenticated by demonstrating, substantiating, validating, a claimed identity of user, device, or another entity in an information or communication systems

E-Commerce Act, R.A. 8792, Chapter 2 continuation

- Among other Chapters and Sections.
- Extent of liability of service provider (Section 30)
- Obligation of confidentiality (Section 32)

E-Commerce Act, R.A. 8792, Penalties (Section 33)

- Hacking or cracking
- Piracy
- Violations of the Consumer Act, R.A. 7394
- Maximum penalty of P1,000,000.00 or 6 years of imprisonment
- Check implementing rules and regulations or IRR for relevant info

Rules on Electronic Evidence

- Section 1. Scope.
  - These rules shall apply whenever an electronic data message is offered or applied in evidence
- Section 2. Cases. All civil actions and proceedings, as well as quasi-judicial and administrative cases
- Section 3. Application of the other rules on evidence. Pertinent evidence of statues containing rules on evidence shall apply
  - Check revised penal code and special penal laws

Rules on Electronic Evidence continuation

- Electronic documents
- Best evidence rule
- Authentication of electronic evidence
- Electronic signature
- Evidentiary weight on electronic documents
- Business records as exception to the hearsay rule
- Method of proof
- Examination of witness
- Audio, photographic, video and ephemeral evidence
- Effectivity

Data Privacy Act, R.A. 10173

- An Act protecting individual personal information and communications systems in the government and private sector
- Creates National Privacy Commision

Data Privacy Act, R.A. 10173 continuation

- Section 2. Declaration of policy. It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth
  - The State recognizes the vital role of ICT in national building and its inherent obligation to ensure that personal information in information and communications systems in the government and private sector are protected and secured

Data Privacy Act, R.A. 10173 continuation

- Section 4. Scope.
  - This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or establish in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines

Data Privacy Act, R.A. 10173 continuation

- This Act does not apply to:
  - Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including
    - Title
    - Salary range
    - Document prepared in the course of employment
    - And so forth

Data Privacy Act, R.A. 10173 continuation

- Chapter 5. Penalties
  - Section 25. Unauthorized processing of personal information and sensitive personal information.
    - Unauthorized processing of personal information – 1 year imprisonment to 3 years and a fine of not less than P500,000.00 but not more than P2M
    - Unauthorized processing of personal sensitive information – 3 to 6 years imprisonment and P500,000.00 but not more than P4M

Data Privacy Act, R.A. 10173 continuation

- Section 26. Accessing personal information and sensitive personal information due to negligence.
  - Personal information due to negligence – 1 to 3 years of imprisonment and P500,000.00 up to P2M fine
  - Personal sensitive information due to negligence – 3 to 6 years of imprisonment and P500,000.00 to P4M fine

Data Privacy Act, R.A. 10173 continuation

- Among other sections pertaining to penalties includes:
  - Section 27. Improper disposal of personal information and sensitive information
  - Section 28. Processing of personal information and sensitive information for unauthorized purposes
  - Section 29. Unauthorize access or intentional breach
  - Section 30. Concealment of security breaches involving personal sensitive information
  - Section 31. Malicious disclosure
  - Section 32. Unauthorized disclosure
  - And so forth

Cybercrime Prevention Act, R.A. 10175

- Section 2. Declaration of policy. The State recognizes the vital role of information and communications industries such as
  - content production,
  - telecommunications,
  - broadcasting,
  - electronic commerce, and
  - data processing, in the nation's overall social and economic development.

Cybercrime Prevention Act, R.A. 10175 continuation

- The State also recognizes the importance of providing an environment conducive to the
  - development,
  - acceleration, and
  - rational application and exploitation of information and communications technology (ICT) to attain free, easy, and
  - intelligible access to exchange and/or delivery of information; and
  - the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and
  - the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts.

Cybercrime Prevention Act, R.A. 10175 continuation

- The State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their
  - detection,
  - investigation, and
  - prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

Cybercrime Prevention Act, R.A. 10175 continuation

- Chapter 2. Punishable acts. Section 4. Offenses against CIA deuce-ace:
  - Illegal access
  - Illegal interception
  - Data interference
  - System interference
  - Misuse of devices
  - Cybersquatting

Cybercrime Prevention Act, R.A. 10175 continuation

- Computer-related offenses
  - Forgery
  - Fraud
  - Identity theft

Cybercrime Prevention Act, R.A. 10175 continuation

- Content-related offenses
  - Cybersex
  - Child pornography (The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009)
  - Unsolicited commercial communications
  - Libel (protested provisions)

Cybercrime Prevention Act, R.A. 10175 continuation

- Section 5. Other offenses
  - Aiding and abetting
  - Attempt

Cybercrime Prevention Act, R.A. 10175 continuation

- SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided,* That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Cybercrime Prevention Act, R.A. 10175 continuation

- Chapter 3. Section 8. Penalties
  - Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Cybercrime Prevention Act, R.A. 10175, Section 8

- Penalties
  - Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

Cybercrime Prevention Act, R.A. 10175, Section 8 continuation

- Penalties
  - If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

Cybercrime Prevention Act, R.A. 10175, Section 8 continuation

- Penalties
  - Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

Cybercrime Prevention Act, R.A. 10175, Section 8 continuation

- Penalties
  - Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Cybercrime Prevention Act, R.A. 10175, Section 8 continuation

- Penalties
  - Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

Cybercrime Prevention Act, R.A. 10175, Section 8 continuation

- Penalties
  - Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

Cybercrime Prevention Act, R.A. 10175, Sections

- Corporate liability (Section 9)
- Law enforcement authorities (Section 10)
- Duties of law enforcement authorities (Section 11)
- Realtime collection of traffic data (Section 12)
- Preservation of computer data (Section 13)
- Disclosure of computer data (Section 14)

Cybercrime Prevention Act, R.A. 10175, Sections continuation

- Search, seizure and examination of computer data (Section 15)
- Custody of computer data (Section 16)
- Destruction of computer data (Section 17)
- Restricting or blocking access to computer data (Section 19)
- Noncompliance (Section 20)
- General principles relating to international cooperation (Section 22)

Cybercrime Prevention Act, R.A. 10175, Jurisdictions

- Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act
- Violation committed by a Filipino national regardless of the place of commission

Cybercrime Prevention Act, R.A. 10175, Jurisdictions cont'n

- Committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines
- Designated special cybercrime courts manned by specially trained judges

Cybercrime Prevention Act, R.A. 10175, Competent Authorities

- Section 23. Department of Justice
  - Created within the department an Office of the Cybercrime
- Section 24. Cybercrime Investigation and Coordinating Center
  - Inter-agency body
  - Under the administrative supervision of the Office of the President
    - Policy coordination among concerned agencies
    - Formulation and enforcement of the national cybersecurity plan

Case Studies

Readings and Discussions

Case Studies: Readings & Discussions

- Important notes:
  - Readings are given every last meeting of the week
  - Discussions are dealt with beginning every first meeting of the week

Case Studies: Readings & Discussions

- CSI Without A Clue
- Legal Aspects of Digital Forensics
- Access Device Act of 1998, R.A. 8484
- The Legal Argument of Opensource Tools in DF
- Rules on Electronic Evidence (PH) and the Analysis Made by American Bar Association's (ABA) Asia Law Initiative

Philippine Cases

Digital Forensics Effort PH

- 2004, 1st cybercrime conviction (PNP-CIDG)
- 2006, 2nd cybercrime conviction (NBI)
- What laws have been used? Cybercrime Prevention Act was ratified in 2012? Et al.