

# A Perspective on Technology Education for Law Students

Anthony G. Volini

DePaul University College of Law

Reg. Patent Attorney, CIPP/US, CIPP/E, CSXF

M.S. Cybersecurity (Networking & Infrastructure Conc., Expected 2020)

# About me

- Completed 13 courses toward my MS in Cybersecurity
- Spearheaded DePaul's IT cross listing initiative for JD students
- Teaching at DePaul nearly 15 years:
  - **Data Privacy Law: US & EU** (interdisciplinary)
  - **Legal Responsibilities in IT** (law students + computing students)
  - **Cybersecurity Law** (under development)
  - Patent & Trademark drafting
  - IP Licensing drafting
  - IP Legal Writing
  - Innovation & the Law at 1871 & 2112

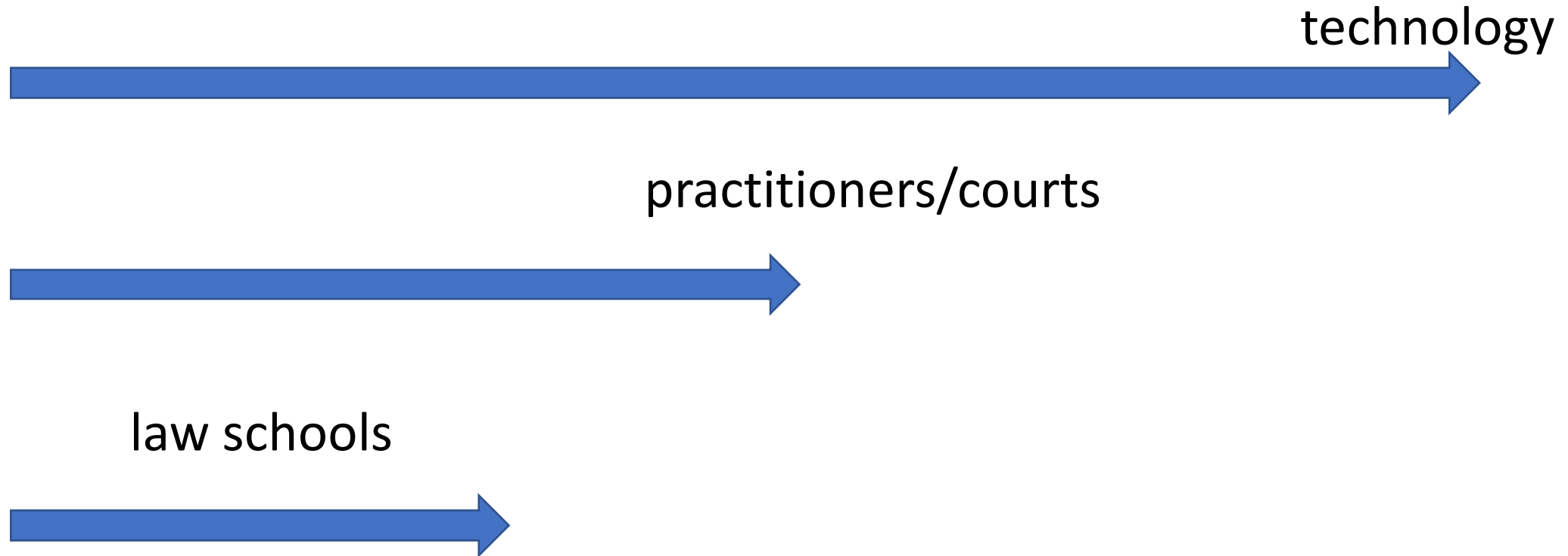
# The need for tech education for future lawyers (analogy to Spanish)

- Imagine a marketplace where many clients are speaking Spanish and most lawyers don't speak Spanish
- Imagine most legal educators don't speak Spanish
- Imagine the number of Spanish speaking clients is growing at an exponential rate
- Imagine significant growth of **nonlawyer** Spanish speaking professionals responding to the need for legal services in this Spanish speaking marketplace
- Imagine the opportunities for Spanish speaking lawyers
- Imagine the necessity for law students to learn Spanish

# Obviously, I'm talking about IT

- But, I'll stick with the analogy (and weave in and out of it)
- **The solution:** teach law students Spanish and determine the appropriate depth of Spanish education while also training students for the bar.
- We probably can't keep up with tech (next slide), but we can give law students a basic foundation in tech for future learning

We're unlikely to catch up with technology any time soon!



# Tech seems to grow at an exponential rate

- Best evidence = running out of IPv4 address space
  - cnn.com = 151.101.193.67
  - Depaul.edu = 140.192.5.61
- These are IPv4, dotted quad/dotted decimal IP addresses. Every computer has one. These computers are cnn's and depaul's web servers.
- IPv4 was designed in the early 1980's with a theoretical address space of nearly 4.3 billion possible addresses\* (US population 1980 roughly 225 million and smartphones, IoT not contemplated).
- In the near future, we will run out of IPv4 addresses, so IPv6 has been developed.

\* (Each quad could theoretically have a value between 0 and 256, so the math is  $256^4$  addresses.)

Optional = perform nslookup on cnn.com

# We can't keep up: law schools have limitations

- We need to continue teaching historical case law/traditional legal principles because they're essential
- We probably can't turn a law school into an IT school and expect students to pass the bar
- But, we can do something! Provide some foundation in IT: language and concepts. (the more the better)

# Why the language analogy?

- **IT is its own language** and most businesses speak IT
- **Fear response** when attorneys confronted with foreign language (xenoglossophobia = fear of foreign languages)
- IT has many areas or dialects. Learning some areas of IT makes other areas a quick study



# tech education will help students

- I'm asking this audience to accept the proposition that tech education is necessary for law students to thrive:
  - HIPAA
  - GLBA & FCRA
  - FTC Act
  - GDPR
  - CCPA (and other developing state law)
  - Criminal Privacy statutes (e.g., ECPA/SCA, CFAA)
  - ABA rules 1.1 and 1.6
  - NC and FL now (2019) require 1 or more hours of tech CLE

# A little more on the need

- Peter Swire has discussed the need for a new middle layer of professionals, knowledgeable in both law and tech.\*
- These folks liaise between upper management and the technologists.
- They can be lawyers or non lawyers.
- In his proposed **Cybersecurity Pedagogical Framework**, he proposes adding layer 8 (organization), layer 9 (government), and layer 10 (international) to the existing OSI layers 1-7 of computing.
- OSI Layers 1-5 are essentially networking layers and layer 7 is the application layer (computer programs)

\* Peter Swire, *Privacy and Security: A Pedagogic Cybersecurity Framework*, 81 Comms of the ACM 23, 24, available at <http://peterswire.net/wp-content/uploads/Pedagogic-cybersecurity-framework.pdf> (Oct. 2018).

# OSI Model





## Open System

## Interconnection model.

-An abstract model for understanding computing.

-Top layer (layer 7) is the application layer (software applications/programming)

-Lower layers (1-5) focus on networking

	High Intelligence (layer 7): <b>Software</b> interacting with <u>user</u>
Gateways (e.g., an internet facing router), firewalls, PC functions	Medium to High intelligence (layers 4-6): protocols that negotiate communication (e.g., max. fragment size, permitted traffic) between a computer on one network and a computer on another network.
	Medium Intelligence (layer 3): a <b>router</b> deciding whether to send data outside of the local network
	Lower intelligence (layer 2): a <b>switch</b> that can send data to all local machines connected to it or individual machines
	Lowest intelligence (layer 1): electrically conductive material to transmit signals ( <b>ethernet</b> or fiberoptic cable)

# Continuing the analogy

- Q: How much Spanish education would benefit students in my hypo?
- Short answer: the more the better.

Other answers:

- One course in basic Spanish is better than none in this Spanish-dominated market.
- More is even better.
- How about **some level of fluency**?

# Depth of Spanish education

- Hypothetical Bachelor's of Spanish sequence:

- Spanish Basics 1

- Spanish Basics 2

- Intermediate Spanish 1

- Intermediate Spanish 2

- Several Advanced Spanish courses



After completing an intermediate course, students might be ready for Spanish Immersion or study abroad experiences?

# How much for a foundation?

- 3-6 IT courses might provide a foundation for further learning outside of law school (complete intermediate Spanish 1 or 2)?
- Intermediate Spanish course is not enough for fluency, but it **provides a foundation** for students to more easily achieve fluency.
- My own experience: After 5-6 IT courses, I was in a position to have somewhat intelligent discussions with technology executives. (I had enough background in terminology and concepts to understand and ask meaningful questions.)
- Law schools can allow some IT coursework to **provide a basic foundation** in IT without compromising the essential legal education.

# Spanish Immersion?

- A conference with technologists and lawyers?
- Placing law students and IT students in the same course?

# Hire a translator?

- 2019: Georgetown law school hired a nonlawyer computer scientist, Professor Matt Blaze, to join its full-time law faculty.
- Professor Paul Ohm: first such hiring of a nonlawyer at any law school in the country. Professor Blaze “‘will teach innovative, interdisciplinary courses at the law school, including Technology of Surveillance and Electronic Voting Technology and Law,’ says Ohm



# A semester abroad?

- Encourage tech focused **internships** at law firms, in house positions, consulting firms, technology firms

# Spanish for lawyers course?

- Various law schools offer **programming for lawyers** courses. This is great.
- Another option is **cross listing** introductory programming and networking (and/or other tech courses) from a University's computing school (as DePaul has done)
- Benefit = law students practicing communication with technologists

# “Spanglish” ?

- Encourage interdisciplinary law courses with a tech component (mix law and tech).
- Teach **and test** tech concepts as an area of competence.
- Topics in my data privacy law course:
  - How the internet works (http vs https, client-server model, ports, network address translation, sessions/TCP handshake), OSI layers, firewalls, DMZs, local encryption, public key encryption, layered defense strategies/Defense in Depth; CIA triad (along with non repudiation), cookies (persistent vs. session, 1<sup>st</sup> party vs. 3rd parties), IAAS, PAAS, SAAS, VPNs, DNS.
- Topics in spring 2020 cybersecurity law course:
  - digital forensics and security by design (e.g., software, servers)

# My proposed curricular priorities

- 1<sup>st</sup> priority = provide “under the hood instruction” in **networking & programming** (with an emphasis on security)
- 2<sup>nd</sup> priority = add coursework/instruction on **any other desired areas** of tech (eDiscovery, forensics, project management, blockchain, AI, etc.)
- 3<sup>rd</sup> priority = encourage interdisciplinary law courses with a tech component. Teach and test tech concepts as an area of **competence**.

1<sup>st</sup> priority = provide “under the hood instruction” in **networking & programming** (with an emphasis on security)

- Millennials often understand user-side of tech, but not the under the hood concepts of networking and programming
- Programming & Networking instruction (i.e., how computers work and how they talk to each other) provides a foundation in OSI layers 1-7, which ties in to Swire’s model
- It’s possible to learn networking and programming without security emphasis (so make sure security is emphasized given its legal importance)

# 1<sup>st</sup> priority (networking and programming)

- Melanie Reid: students with a computer science degree may be better prepared for legal practice than other students.\*
- **Question:** Why? (they're not doing the IT work)
- **Answer:**
  - they have tech fluency to handle legal tech issues
  - Good position to manage legal tech issues, participate: brainstorming of software development (e.g., security by design, legal process design, other issues), assessing incident response, data breach suits, cybersecurity compliance (HIPAA, GLBA, NIST, GDPR), etc.

\*Melanie Reid, A Call to Arms: Why and How Lawyers and Law Schools Should Embrace Artificial Intelligence, 50 U. TOL. L. REV. 477, 490 (2019)

2<sup>nd</sup> priority = add coursework/instruction on **any other desired areas** of tech (eDiscovery, forensics, project management, blockchain, AI, etc.)

- Reinforce/Supplement the networking and programming concepts
- Offer other tech courses that students and faculty are interested in (depends on who is available to teach particular courses)

3<sup>rd</sup> priority = encourage interdisciplinary law courses with a tech component. Teach and test tech concepts as an area of **competence**

- **Cybersecurity Law course** (under development): digital forensics emphasis and software security by design (along with the law)
- **My Data Privacy Law: US & EU course** (approx. 25% tech content)
  - Cover all sectors of US privacy + GDPR and EU institutions/history
  - Week 1: how the internet works from powering on laptop, logging onto enterprise network, visiting remote web server
  - Tie in a variety of other tech concepts throughout the course (relate to the law, e.g., FTC v. Wyndham)



# Keeping up with the marketplace:

## side Note on Agile Project Management

- Law schools require radical change to adapt to the new marketplace.
- Law schools explore this radical Agile management model?
- Per Gartner, by 2023 most businesses are expected to use Agile.\*
- What makes it radical?
  - Small, empowered, autonomous teams
  - Adaptive and iterative project management (rather than approval of all details up front)
  - Less bureaucracy, fewer meetings, higher employee satisfaction
  - Perceived by traditional managers as radical anarchy!

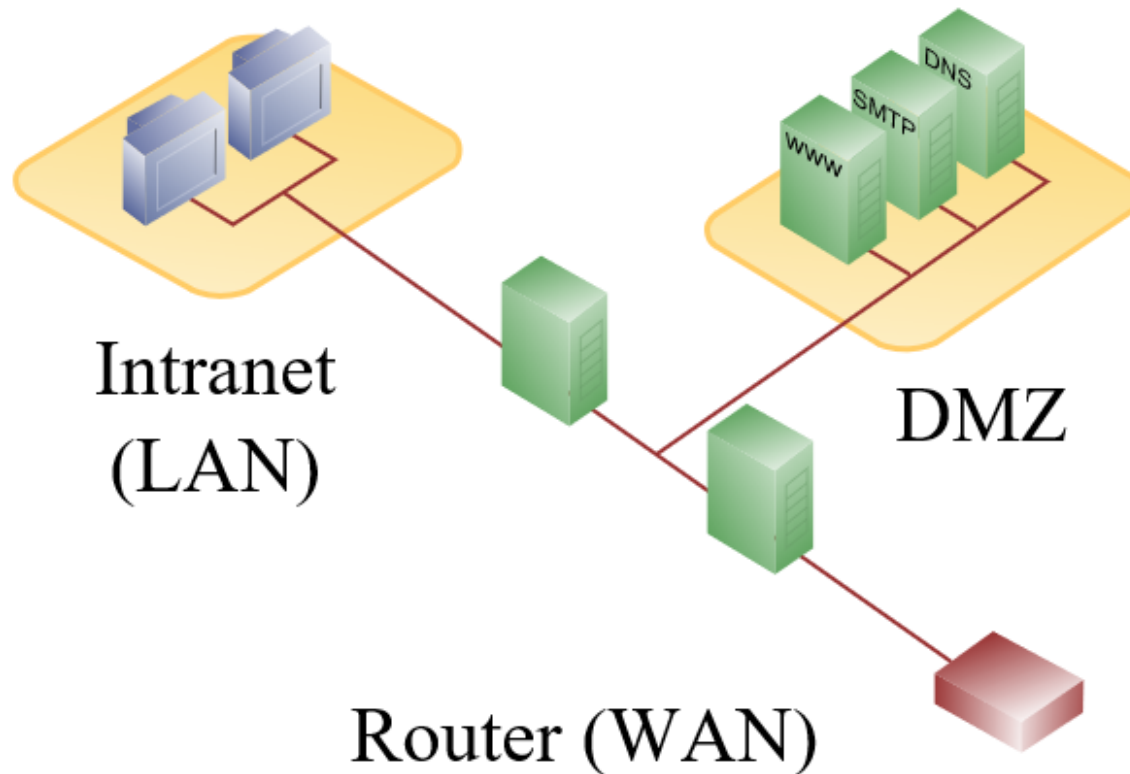
\* <https://www.gartner.com/smarterwithgartner/gartner-predicts-3-digital-business-impacts-on-ppm/>  
Seventy-one percent of organizations report using agile approaches for their projects sometimes, often, or always. <https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2017.pdf> at page 6.

# Survey tech concepts (time permitting)

- If out of time, field questions

Using visuals\* and exploring tech details (slide from my Data Privacy course)

DMZ Option 1: insert servers (e.g., web server) between two firewalls  
(public domain image)



\* James B. Levy, *Teaching the Digital Caveman: Rethinking the Use of Classroom Technology in Law School*, 19 Chap. L. Rev. 241, 274-75 (2016) ("The best way to teach and learn any subject is to employ the methods that are most compatible with the desired outcome . . . Vision is by far the brain's most dominant sense . . .").

- Survey a few tech concepts (that relate to the law)
  - Networking concepts
  - Digital Forensics & Metadata
  - Forensic images and MD5 hash values and deletion

# Metadata

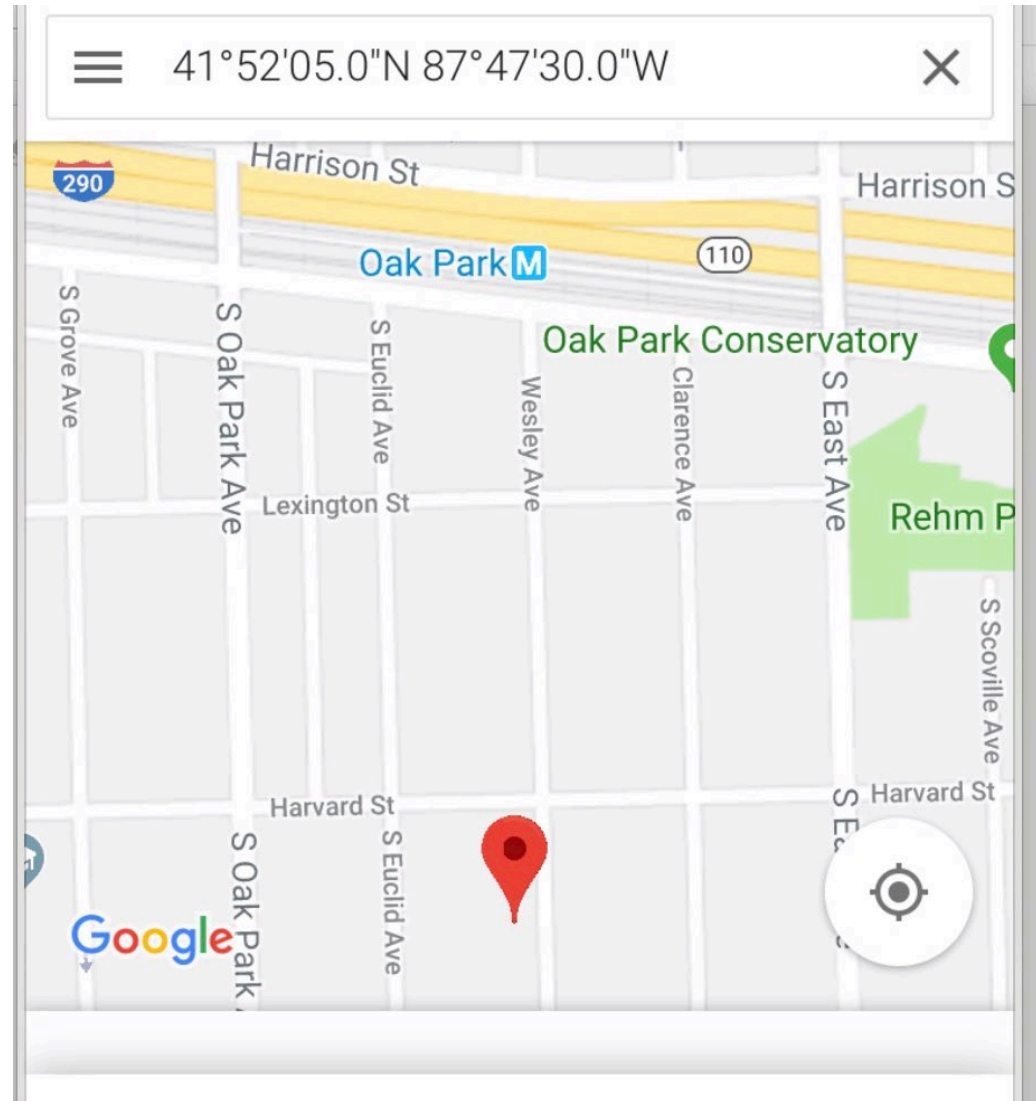
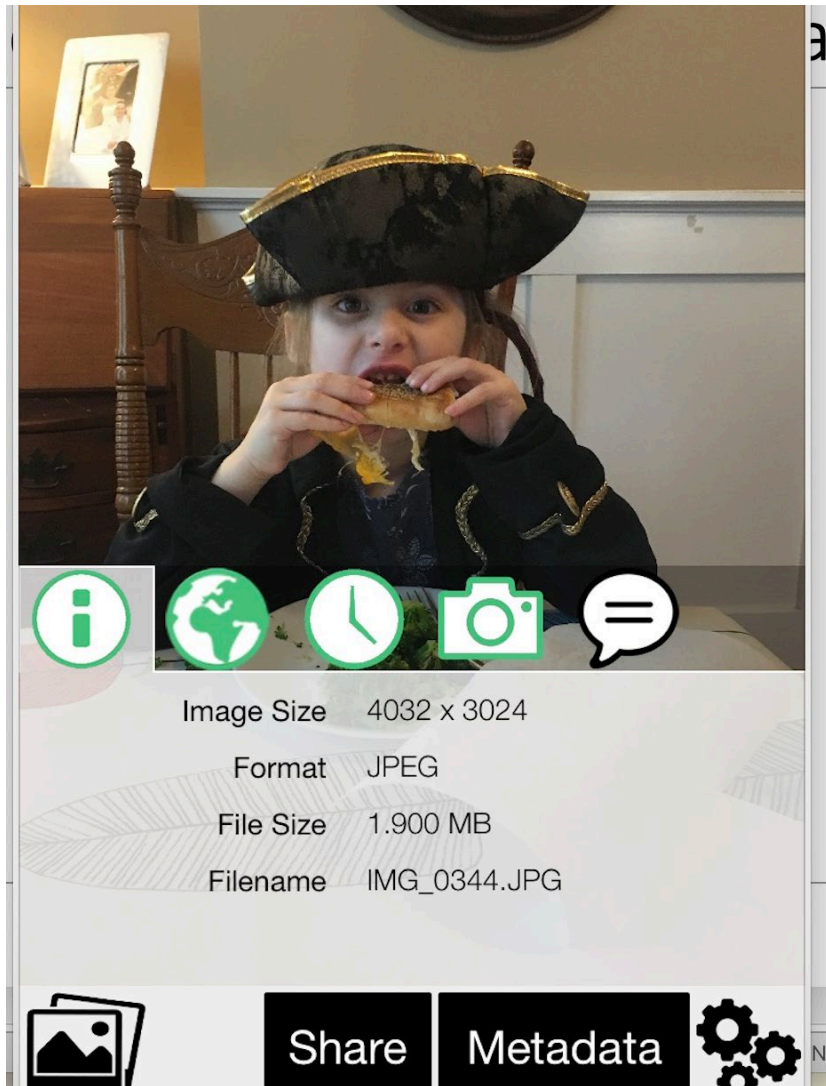
- What is it? Typically, it's data about a file. Date created, date modified, author, GPS location of a photo.
- Why should lawyers care? Good idea to include metadata in a discovery request for ESI (form of production).\*

\* <https://www.lawtechnologytoday.org/2017/08/e-discovery-request-youre-requesting/>

# Metadata-Picture of my daughter



# Metadata of the picture: from a free iPhone App



# Side note: John McAfee's location in South America was discovered via photo metadata

## Fugitive John McAfee's location revealed by photo meta-data screw-up

03 DEC 2012 17

iOS, Law & order, Mobile

× Don't show me this a

Get the latest security news in your inbox.

you@example.com

Subscribe





# Privacy question: Metadata

- Assume your client operates a dating website where users upload photos of themselves.
- What do you advise your clients regarding photo metadata? Can you imagine a scenario that could create liability regarding photo metadata?

# Litigation question: Metadata

- How could photo metadata (e.g., GPS) be useful in a civil or criminal action?
- <https://ediscovery.co/ediscoverydaily/electronic-discovery/metadata-plays-key-role-10-8-million-whistleblower-lawsuit-verdict-ediscovery-case-law/> (discussing how metadata in a wrongful termination whistleblower suit was used to show that the employee's performance evaluation was created a full month after his termination.)
- How about attorney billing records issue?

# MD5 Hash values

- What's an MD5 hash value?

It's a unique value that's generated by an algorithm that assesses data (e.g., an individual file or a forensic image/copy of an entire hard drive)

- Why should lawyers care?

- Time of collecting forensic evidence, the forensic examiner records the MD5 hash value of the data and saves an extra copy of the data before examining the data.
- The saved copy of the data has an MD5 value that matches the MD5 value at the time of collection, negating a theory that the forensic examiner changed the data during the analysis. (The other side can repeat the same analysis on the saved copy and arrive at the same conclusions.). [Chain of Custody-evidentiary concept]

# MD5 Hash value = digital fingerprint

- Q1: Assume I take an MD5 hash value of every computer in the state of Illinois. Will every computer have a unique MD5 hash value?
- Yes. (It's Lottery odds to have two computers match.) A very small difference in the data (e.g., even metadata: date modified) creates a significant difference in MD5 value.
- Q2: Assume I save a Word doc and then generate an MD5 value for it. Next, I open the doc, change a period to an exclamation point, and save again. Will the MD5 value change?
- Yes.

# Collection

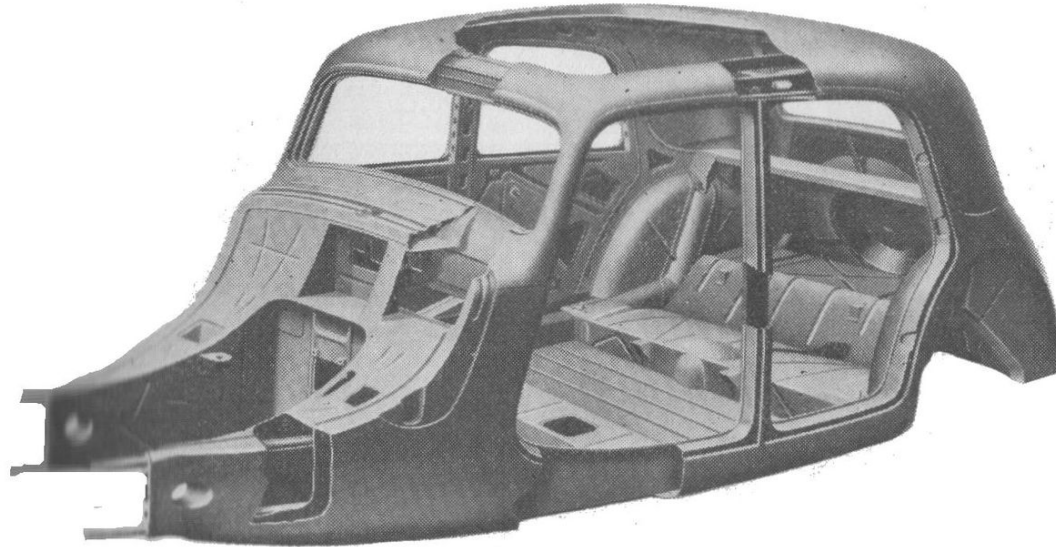
- Assume you are a forensic examiner. You arrive at a crime scene and notice the victim's laptop is on/logged in. Should you (a) power off the laptop and take it back to the police station for analysis or (b) immediately collect a forensic image?

- The correct answer is to take a forensic image for various reasons:
  - If the laptop is password protected, you may struggle with brute forcing it back open after restart and local encryption might be turned on
  - Any data in volatile RAM memory will likely be deleted upon restart (sometimes it survives during laptop hibernation, but unlikely after restart)

# Firewalls

- What's a firewall in an automotive context?

FW = a safety barrier





# FW in computing context

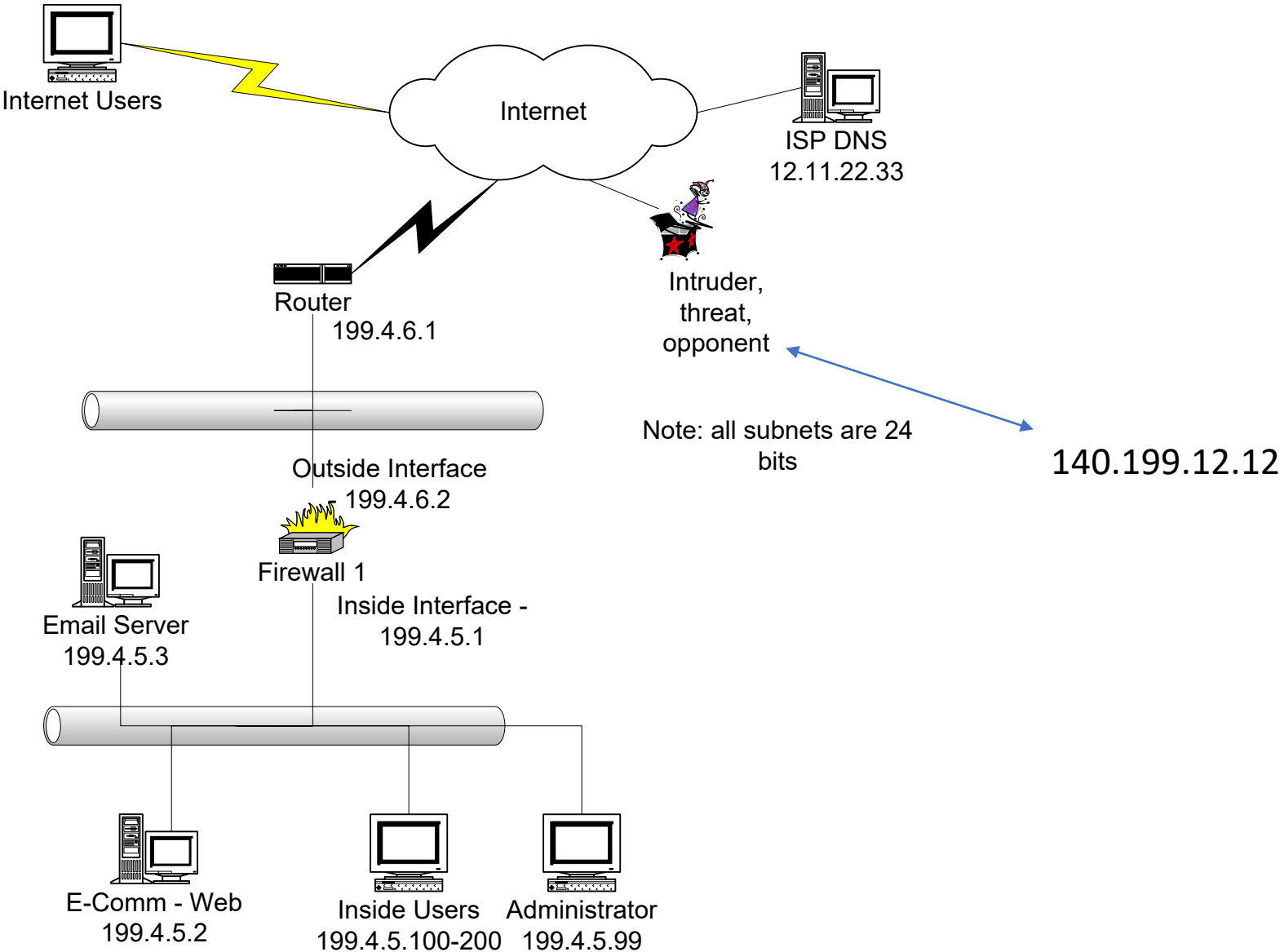
- A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communication.
  - **Host based firewall:** this runs as software on your laptop. You should check your laptop to make sure the firewall is turned on and running so that it implements default safety settings. (Microsoft's firewall will block traffic from untrusted sources-hopefully! It ideally also blocks outsiders from gaining administrative control of your laptop.)
  - **Firewall appliance:** this is a common implementation in an enterprise environment. The firewall appliance is configured by IT/security personnel to allow or reject particular types of **ingress** or **egress** traffic, depending on a variety of factors (e.g., sensitivity of the data, business needs, etc.)

# Let's look at an enterprise network topology

- In the next slide, we'll see a simplified network topology.
- A **router** that connects the enterprise network/**LAN** (local area network) to the internet
- A **firewall** located between the company's inside equipment and the router (much like the automotive analogy)
- Internal devices located behind the firewall (e.g., company desktops, webserver, etc.)

# Simple Firewall Rule Example

My-AC-store.com E-Commerce Infrastructure



- The firewall rules can block the problem IP address, but allow other traffic.
- The **order** of firewall rules is important because they are executed in order. Consider the following conceptual rules:
  1. Allow all internet traffic to the ecommerce public webserver
  2. Reject any traffic from rogue IP address 140.199.12.12
  3. Reject all other traffic not permitted above
- These rules are wrong.
- The solution is to set rule #2 as rule #1.
- Side note: The final firewall rule is typically a default deny all rule at the end to block any other traffic not previously permitted.
- Regular auditing of security controls is important to see if the controls are working properly.

## FWs (cont.)

- Firewall rules are much more involved than my simple example. There are often many rules, and they need to be updated regularly in response to evolving threats. The rules need to be tested regularly. Large organizations will often have multiple FWs to manage.
- Also, while FWs typically focus on blocking outside threats, they can potentially be configured to inhibit insider threats. For example, you can write a firewall rule that prohibits **internal devices** from visiting a known malicious site. This is actually required with a **stateful** firewall: you need to write rules in both directions so that you can protect against wherever the traffic initiates: for example, an outside threat from the bad IP address trying to get in and an inside user perhaps trying to go out to that bad IP address (perhaps unwittingly in response to a phishing attack).