# DRAFT

**JULY 26 2019**

A PERSPECTIVE ON TECHNOLOGY EDUCATION FOR LAW STUDENTS

Anthony Volini

*Law schools continue to appreciate the importance of technology awareness for law students practicing in the 21st Century. As law schools have a desire to educate law students on technology, there is need for determining curricular priorities in this relatively new endeavor. This essay thus proposes curricular priorities to help law students face the challenges of an increasingly tech-driven legal marketplace and enable them to improve on bridging the communication gap between lawyers and technologists.*

*This essay proposes a set of curricular priorities for teaching tech to law students and analogizes learning technology to learning a second language. It provides specific examples (i.e., technology vignettes) that may be incorporated into a tech law focused course, along with comments on specific tech topics that may be incorporated into a data privacy course or other tech law course.*

*A major emphasis of this essay is that law students can benefit from learning the backend or "under the hood" instruction as opposed to merely user side tech education. Law students likely benefit from learning user-side tech (e.g., practice tools), and law schools can and should continue providing this education. However, I propose that a robust tech curriculum for law students prioritizes addressing under the hood concepts of networking and programming to facilitate a deeper understanding of Information Technology (IT) as opposed to solely user-side tech education. A variety of law schools have programming for lawyers courses, which is consistent with my proposal. However, schools could also address networking concepts to provide students a more complete foundational understanding of the OSI layers consistent with Peter Swire's Cybersecurity Pedagogical Framework. Such knowledge should be a major asset as lawyers will need to work with IT professionals when addressing matters such as cybersecurity/data privacy, tech contracts, legal process design, security by design, and other tech law issues.*

*I propose a curricular model with three priorities (perhaps offered in an elective format for optimal flexibility):*

*(1) networking and programming instruction*

*Ideally, law schools, as a first priority, might strive to provide law students with coursework addressing under-the-hood concepts of programming and networking. The tech concepts should be taught and tested as an area of competence. (Some law schools already provide programming for lawyers courses.) Coursework in networking and programming should include relevant security concepts in combination with the fundamentals given the increasing importance of cybersecurity/privacy law. Addressing these core two areas would provide some foundation for understanding OSI layers 1-7 consistent with Swire's model.*

*Besides programming for lawyers courses and the like, another option for educating on networking and programming is by cross listing such courses from a University's computing school.*

*(2) coursework in other areas of tech*

*In addition to coursework addressing programming and networking, law schools could also offer coursework in any other relevant areas of tech, depending on factors such as available instructors and*

*student interest. Such other coursework could address any variety of tech topics, such as legal practice tools, data analytics, digital forensics, systems, security management principles, IT project management, other tech management, such as disaster recovery, etc. Study in these other areas would reinforce or supplement understanding of the OSI layers, and of tech generally.*

*(3) inter-disciplinary law courses with a substantial tech component that is likewise taught and tested as an area of competence*

*As discussed below, law schools are limited in the number of tech courses they can offer students given the importance of training students to pass the bar. However, a law school wishing to provide students with a basic foundation in tech could strive for offering perhaps three to six technology courses (likely focused on technology more than law) to provide them with an "intermediate" level of tech fluency: a foundation for further learning outside of law school. This is akin to providing a student with 3-6 courses in Spanish to achieve an intermediate level of Spanish language proficiency, a foundation for future learning. As technology continues to change, rather than focusing solely on keeping up with the latest changes, law schools can instead focus on providing a basic foundation on how computers operate (i.e., programming) and talk to each other (i.e, networking) so that students can be more adept at understanding new technologies as they evolve.*

**About my journey**

I have been teaching law school full-time since 2005.[1] In 2016, I wondered how I might make myself more relevant in academia. The answer to me was very clear: obtain a technology degree given the growing need for tech savvy lawyers in the marketplace.[2] So, I started pursuing a Masters in Cybersecurity at DePaul (networking and infrastructure concentration). As of this writing, I have completed twelve courses toward the degree and am nearing completion. Several of the introductory computing courses in the program struck me as potentially a great fit for law students, so I successfully lobbied the faculties of DePaul's law school and computing school to allow any upper level JD student to take up to four select IT courses and receive JD credit for same.[3] I believe this is a relatively unique curriculum. While many law schools, including DePaul, offer joint programs (e.g., JD/MS), few law students are willing to simultaneously pursue two graduate degrees (so allowing a few IT courses for JD credit may seem like an attractive option for law students to develop some technology awareness).[4] As a side note, I have not observed other law schools marketing a similar educational opportunity to their students, so I suspect the majority of law schools might not allow --or at least don't appear to actively promote-- this type of interdisciplinary curriculum.

---

[1] I currently teach a variety of courses, including Data Privacy Law: US & EU, IP Licensing (drafting), Innovation & the Law at 1871/2112, Patent & TM Drafting, first year legal research & writing (specialized IP legal writing section), and Legal Responsibilities in IT (co-taught with one of our computing school professors).

[2] I recall meeting with an IT executive around that time who told me that he only hires lawyers who have at least a basic understanding of his company's IT. His small company at the time spent roughly $50,000 per month on legal services.

[3] Those courses include intro to programming; business continuity/disaster recovery; information security management; and legal responsibilities in IT. I worked closely on this initiative with Ellen Gutiontov, Executive Director of DePaul's CIPLIT® (Center for Intellectual Property Law & Information Technology) program at the College of Law.

[4] When I put this curriculum together, I contemplated law students with no tech background and how this curriculum could offer them a basic level of tech fluency.

Besides technology education, I have also obtained several certifications (and I encourage law students to pursue these as well). I have obtained the CIPP/US and CIPP/E data privacy certifications as well as ISACA's Cybersecurity Fundamentals Certificate.[5]

With this background, I began teaching Data Privacy Law: US & EU in the spring of 2019 and experienced tremendous enrollment of 50 students with several on the waiting list. While developing the course, I realized that I needed to provide substantial relevant technology education to accompany the statutes and case law in the course (which I discuss in more detail below).

I started my career as a full-time patent attorney, so this chapter in my career seems to be a continuation of my interest in combining technology with the law.

**Part 1: The need for tech savvy lawyers in the 21st Century**

Much has been written about the need for tech savvy law graduates, and there seems to be a consensus among legal educators that this is important.[6] In this essay, I will minimize arguing that the need exists. However, continued discussion of which tech topics to teach and how to teach them should be valuable as law schools pursue this relatively new endeavor.

A few thoughts to consider on the growing need for tech education are (1) most states have adopted ABA Rule 1.1 that lawyers have technological competence[7], (2) as of 2019, North Carolina and Florida now require technology CLE for attorneys[8], and (3) data privacy legislation is growing and current and future statutes, both state and federal, will have or continue to have express or implied cybersecurity requirements, which lawyers will need to understand.[9]

Renowned privacy law expert Peter Swire has predicted that the future marketplace will have a growing need for a new middle layer of professionals having a combination of law, technology, and business knowledge.[10] [11] These professionals can be lawyers or nonlawyers, and their job is to liaise between

---

[5] I created a YouTube channel to advise a broad audience on how to prepare for these certifications. The playlist is available at https://www.youtube.com/playlist?list=PLhAOJU2XD-IuR-R6_-8yrENL2glqLEg8s

[6] *See, e.g.*, Oliver R. Goodenough, *Developing an E-Curriculum: Reflections on the Future of Legal Education and on the Importance of Digital Expertise*, 88 Chi. Kent L. Rev. 845 (2012); Law Schools Looming Skills Crisis by Mark Cohen at https://www.forbes.com/sites/markcohen1/2019/05/21/laws-looming-skills-crisis/#760ea8bd445c; also by Cohen is DXC is Serious About Legal Digital Transformaiton at https://www.forbes.com/sites/markcohen1/2018/10/08/dxc-is-serious-about-legal-digital-transformation/#2d28b8f33094]

[7] Robert Ambrogi, *Make That 30 States, As Another Adopts Ethical Duty of Technology Competence*, available at https://www.lawsitesblog.com/2018/03/make-30-states-another-adopts-ethical-duty-technology-competence.html (Mar. 14, 2018).

[8] Doug Austin, *A Second State Now has Approved a Technology CLE Requirement for its Lawyers: eDiscovery Trends*, available at https://www.jdsupra.com/legalnews/a-second-state-now-has-approved-a-87363/ (Dec. 7, 2018).

[9] Alfred J. Saikali, *The Developing Landscape of Data Protection Laws and Enforcement Actions*, available at https://www.americanbar.org/groups/litigation/committees/products-liability/practice/2019/the-developing-landscape-of-data-protection-laws-and-enforcement-actions/ (Apr. 9, 2019).

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

[11] Evidence of this growing middle layer in legal systems can be seen in the development of alternative business structures in the UK (i.e., nonlawyers sharing fees with lawyers in the provision of legal services).

technologists and upper level management. For law schools to produce lawyers to fill this middle layer, they would need to teach both technology and business to lawyers.[12] This essay focuses on the technology aspect and not on the business education aspect (the business education aspect could be addressed in some future essay).

Swire has provided a new cybersecurity pedagogical framework that builds upon the OSI model of computing, adding his layers 8-10 to the OSI model's existing layers 1-7.[13] The OSI model is the Open Systems Interconnection model and is a conceptual model for understanding how computers operate and communicate with each other.[14] Often, technologists will use these layers to troubleshoot performance problems. Layer 1 is the physical layer (e.g., 1s and 0s traveling across an ethernet cable).[15] Most IT problems are said to occur at layer 1, which is why help desk personnel routinely first ask whether all cables are installed and the power is on as a starting point for troubleshooting. Layer 2 is the data link layer. In an enterprise network, the data link layer might involve an organization's internal PCs and printers connected by switches.[16] Layer 3 is the network layer. A router is commonly referenced as a layer 3 device, and it makes the decision of whether data needs to be sent out to the internet.[17] Layer 4 is the transport layer and layer 5 is the session layer.[18] These layers establish a communication channel or "session" between two computers. For example, a user's laptop could communicate with a web server, and the two computers could first agree to communicate (i.e., open a "session"), agree on the size of data packets to send each other, and agree on whether to encrypt the data they send to each other (e.g., the https protocol provides for encrypting most data sent between a user's computer/browser and a web server, which increases the difficulty of an eavesdropping attack as compared to http/unencrypted communication). Layer 6 is the presentation layer and is often referred to as the syntax layer. Layer 6 essentially translates data into a usable form for layer 7 the application layer so that the application layer can perform higher level processing on the data.[19] For example, layer 6 might be responsible for decrypting data so that it is usable by a layer 7 software program. Layer 7 is the application layer, which implicates software applications (e.g., Windows 10, Microsoft Word, Internet Explorer, etc.).[20]

---

https://www.chambersstudent.co.uk/where-to-start/newsletter/alternative-business-structures; See Richard Susskind, Tomorrow's Layers (2d ed. 2017) at p. 7.

[12] As a side note, besides teaching tech to law students, my colleague Professor Karen Heart (DePaul College of Computing and Digital media) and I are teaching the law to computing students in IS 482: Legal Responsibilities in IT (accommodating both law and computing students).

[13] 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).

[14] *See generally*, H. Zimmermann, *OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection*, 28 IEEE Transactions on Communications 425, available at https://ieeexplore.ieee.org/abstract/document/1094702/citations (Apr. 1980).

[15] *See generally,* Paul D. Bartoli, *The Application Layer of the Reference Model of Open Systems Communication*, 71 Proceedings of the IEEE 1404 (Dec. 1983).

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

Swire adds layers 8, 9, and 10 (organization, government, and international layers, respectively) to the existing OSI layers 1-7.[21] The brilliance of Swire's model is that it provides a common framework for technologists and lawyers to use, by simply adding human layers 8-10 on top of the existing IT layers. It would seem that professionals operating in layers in 8-10 would need good awareness of layers 1-7, which supports my proposal of priority 1, providing basic instruction in programming (layer 7) and networking (layers 1-5).

In my opinion, Swire's model seems useful not only as a pedagogical framework for teaching cybersecurity but really for any area of technology: any professional communicating with technologists would seem to benefit from deepening her understanding of OSI layers 1-7 when engaged in any management involving technology. For example, medical students could benefit from instruction in the OSI layers if their careers later involve communicating with IT on development of new processes or online tools for improved healthcare.

Law students who have coursework focused on networking (e.g., layers 1-5) and programming (layer 7) will have a better foundation for understanding future technology developments than a law student whose education focuses exclusively on learning about the most recent legal practice tools from a user perspective or from merely studying the impact of a technology on the legal industry. Essentially, a law school that can provide some level of technical training can provide a liberal arts student with a touch of engineering training, enough to be tech conversant, that should benefit them.

Melanie Reid notes that students with a computer science degree may be better prepared for legal practice than other students.[22] This provokes the question of why. The answer is that the CS grad typically has a deep fluency in tech and therefore has the ability to quickly understand client technology issues and ask the right questions. Typically, the CS grad lawyer does not do IT work, but the deep level of tech fluency afforded by the CS degree puts the lawyer in a much better position than other lawyers because of this communication ability as she works on legal issues intersecting with tech. Her role as a tech lawyer is not do the tech work, but instead is to manage the legal tech issues or to perhaps participate on a team in terms of the high level brainstorming of software development (e.g., security by design, legal process design, or other issues).

Law schools are unlikely to fill their classrooms with CS or engineering students anytime soon, so my focus is on the typical liberal arts student and assessing what depth of IT education will enable the law student to have some level of working tech fluency, probably not the same level of fluency as the CS grad, but enough fluency to facilitate rapid tech learning outside of law school. Along these lines, a 30,000 foot level of tech education for law students is inadequate (e.g., one lecture or week covering the OSI layers), and instead a ten to fifteen thousand foot level of instruction is more helpful to achieve some

---

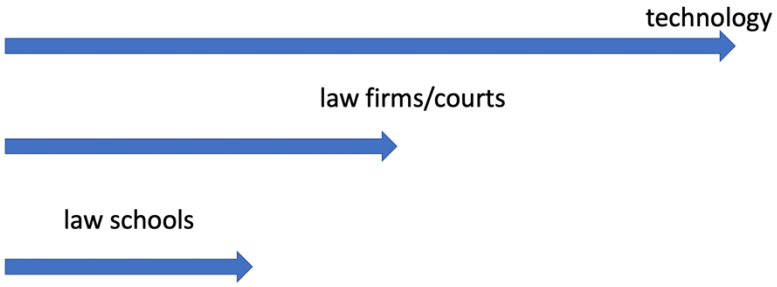
[21] Peter Swire, *Privacy and Security: A Pedagogic Cybersecurity Framework*, 81 Comms of the ACM 23, 24, available at http://peterswire.net/wp-content/uploads/Pedagogic-cybersecurity-framework.pdf (Oct. 2018).

[22] 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): "With the advancement of Al, a computer science degree may be a better preparation for legal practice than a liberal arts degree. Similar to a high LSAT score, a highly technical background may be a harbinger of future success in law school. While there is no necessity for future law students to have a computer engineering or coding background, it is essential these future students feel comfortable with advanced technology so they can adapt and innovate as Al programs evolve."

of the tech fluency of a CS grad (e.g., multiple tech courses, such as my proposed range of three to six tech courses for intermediate fluency). At DePaul, the law school's cross listed introductory level IT courses from the computing school have no prerequisites and essentially function as introductory spanish courses from a tech fluency standpoint.[23] These courses, or the combination of courses, seem a good option to offer some level of depth in terms of IT education.[24]

**Keeping up with tech**

Law schools will continue to struggle to keep up with the marketplace, and perhaps any school in any discipline will struggle to keep up with the marketplace. This is especially the case with technology given its very rapid growth. In fact, even computing schools struggle to keep up with the rapid changes in technology.[25] The image below represents my perception of the lag that may continue indefinitely as courts, law firms, and schools make efforts to catch up with technology:




**The exponential growth rate of technology**

Since its inception, information technology has grown and will likely continue to grow at an exponential rate, making it difficult for lawyers, courts, and skills to keep up. Perhaps the best evidence of technology's exponential growth is that we are running out of IPv4 address space.[26] IPv4 (version 4) was developed in the early 1980s to provide every internet connected computer with a common addressing scheme so that every computer has the same format of address.[27] For example, www.cnn.com has an IP address of 151.101.193.67 and www.depaul.edu has an IP address of 140.192.5.61. These four numbers separated by periods are often referred to as the dotted quad. Each of the four quads can theoretically

---

[23] see FN 3 above

[24] Coding Abilities Becoming Valuable to Lawyers as Blockchain Tech Develops at https://www.law.com/legaltechnews/2018/11/01/coding-abilities-becoming-valuable-to-lawyers-as-blockchain-tech-develops/ ; also about coding: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227967: Legal Education in a Digital Age: Why 'Coding for Lawyers' Matters

[25] Mike Stucka, *Will Education Ever Keep Up with Technology?*, available at https://www.govtech.com/education/Will-education-ever-keep-up-with-technology.html (Oct. 29, 2014).

[26] Geoff Huston, *The Changing Foundation of the Internet: Confronting IPv4 Address Exhaustion*, available at http://wattle.apnic.net/papers/isoc/2008-10/v4depletion.pdf (Oct. 2008).

[27] B. Carpenter *et. al.*, *IPv4 Address Behaviour Today*, available at http://www.hjp.at/doc/rfc/rfc2101.html (Feb. 1997).

have a value of 0-255, thus we could visualize the address space as 0-255.0-255.0-255.0-255. Mathematically, the number of possible addresses is thus $256^4$ or nearly 4.3 billion possible IP addresses.[28] In the early 1980s, 4.3 billion IP addresses likely seemed suitable, considering the U.S. population in 1980 was only about 225 million (this was prior to cars, refrigerators, and smartphones connecting to the internet).[29]

Since the early 1980s, the number of "computers" worldwide has increased exponentially (counting smartphones, tablets, cars, etc.) and is expected to exceed 4.3 billion in the near future. Therefore, IPv6 has been developed, and most computers are now compatible with IPv6 to be ready for future networks relying on IPv6 addressing.[30] (IPv6 addresses are essentially four times longer than IPv4 addresses, and therefore, IPv6 has an astronomical address space of $3.4 \times 10^{38}$ possible addresses.)[31]

Running out of IPv4 address space is an example of the exponential growth of IT since its early days, and the common consensus is that information technology will continue to grow exponentially, not just in terms of additional computers in the IoT era but also information technology generally, such as increased usage of AI.[32]

**Law schools are unlikely to keep up with the exponential growth of tech, but what can be done?**

Legal educators, by necessity, need to look backwards when teaching the law. Rather than addressing novel legal issues presented this week by a client, law faculty wait for developments in case law as one major source of their teaching. Essentially, the sequence of analysis is that clients have a new legal technology issue, their lawyers struggle with the new issue, courts then eventually struggle with that issue, and finally law faculty review issue judicial opinions on the issue and integrate same into their teaching.

Law schools will need to continue teaching historical case law/traditional legal principles because they are essential for lawyers to understand legal issues in our common law system. Further, a law school cannot turn itself into an IT school and expect students to pass the bar.

All that being said, law schools can do something in terms of allowing students to achieve some basic, foundational understanding of IT prior to graduating. At a minimum, law schools can allow students to take several tech-focused elective courses (as described above) either in the law school, at a computing school, or some combination of the two.

In line with Swire's model, I propose that law schools look for ways to educate law students on layers 1-7 of the OSI model to provide sufficient awareness for them to manage his layers 8-10. As discussed

---

[28] Each quad can have a value between 0 and 255, which is 256 possible numbers (counting 0).

[29] https://simple.wikipedia.org/wiki/1980_United_States_Census

[30] See https://www.fcc.gov/consumers/guides/internet-protocol-version-6-ipv6-consumers, noting "most personal computer operating systems support IPv6."

[31] Stanford L. Levin, Stephen Schmidt, *IPv4 to IPv6: Challenges, Solutions, and Lessons*, 38 Telecommunications Policy, 1059 (Dec. 2014).

[32] Melanie Reid (Lincoln Memorial), A Call to Arms: Why and How Lawyers and Law Schools Should Embrace Artificial Intelligence, 50 U. Tol. L. Rev. 477 (2019).

earlier, this would require first curricular priority of offering some training on networking (i.e., layers 1-5), computer programming (mainly layer 7).

In a sense, while IT changes and evolves rapidly, the foundational concepts remain largely the same. Therefore, providing a basic foundation in networking and programming is helpful because the fundamental concepts, most of which were developed decades ago, will stay the same.[33]

**Keeping up: a side note on agile management**

As law schools consider how to adapt to technology changes in the legal marketplace, they could explore an Agile management approach that is popular in a variety of industries.[34]

By 2023, Gartner predicts that Agile Portfolio and Project Management will become the dominant approach for effective enterprise change and outcomes in the business world.[35] Companies, schools, and teams across industries today are differentiating themselves by adopting agile successfully and making it a competitive advantage.[36] Law schools could explore, likely with assistance from a consultant, how Agile project management could contribute to faster and more efficient adaptation to changes in the marketplace. "Some executives seem to associate agile with anarchy (everybody does what he or she wants to)." Therefore, law school leaders might likewise initially view Agile as too radical to implement in a law school. However, if law schools require radical change to adapt to the marketplace, it seems prudent to at least explore the possibility of implementing it.

Agile focuses on incrementally and adaptively pursuing a goal rather than having all details spelled out up front.[37] It focuses on facilitating collaborative, empowered teams through adaptive planning and continuous improvement practices, and by trusting teams rather than micro-managing them and by striving to reduce meetings. It is reported that Agile tends to support a high level of employee satisfaction and productivity with its reduction in bureaucracy.[38]

According to the Harvard Business Review, prospective employees of today are demanding Agile ways of working and being engaged with.[39] Achieving the benefits Agile typically requires a radical cultural change in the way that we think about and perform our work. Pivoting to embrace this Agile way of thinking and performing work seems worth exploring as many have written about the need for radical change in law schools.

Certainly, adopting a flexible, agile approach to changing curriculum and other administrative goals would present some challenges to law schools as many law schools have a tendency to make decisions by

---

[33] *See, e.g.,* Wesley M. Johnston, J.R. Paul Hanna, & Richard J. Millar, *Advances in Dataflow Programming Languages*, 36 ACM Computing Surveys 1 (Mar. 2004).

[34] 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.

[35] https://www.gartner.com/smarterwithgartner/gartner-predicts-3-digital-business-impacts-on-ppm/

[36]

[37] *See, e.g.*, Enric Senabre Hidalgo, *Management of a Multidisciplinary Research Project: A Case Study on Adopting Agile Methods*, 14 J. of Research Prac. 1 (2018).

[38]

[39] https://hbr.org/2016/05/embracing-agile

faculty vote. That being said, exploring the Agile approach with a skilled consultant might produce some potential benefits.

**A thought about study after (or outside of) law school**

The focus of this essay is on what law schools can do in terms of tech training for students to prepare them for practicing in the 21st century. However, some thought can be given to what law students and law school graduates can do outside of law school to increase their tech fluency.

A practicing lawyer can certainly take tech focused CLEs. Also, lawyers and law students could perhaps take an online IT course from a local community college. In fact, I have advised a couple of law students recently to take an online digital forensics course over the summer as a way to increase tech awareness (forensics is a wonderful area of study for lawyers given its importance in eDiscovery and incident response).[40]

Students and attorneys can also consider private certifications as a way to demonstrate technology awareness on their resumes. (As a side note, I have a YouTube playlist with videos discussing how to prepare for various certifications).[41] Two entry level tech certifications that might be attractive are: (1) ISACA's Cybersecurity Fundamentals Certificate (CSXF) and (2) IAPP's Certified Privacy Technologist Certification. Students and lawyers could also explore a basic certification in digital forensics and/or eDiscovery, but I have not explored these in depth. Regarding the Cybersecurity Fundamentals Certificate (CSXF), this is a wonderful starting point to learn about cybersecurity concepts (or it's a good way to supplement and/or reinforce particular concepts from other coursework). This certificate is specifically designed for folks with limited technology background, it has a fairly low cost (roughly $200 as of this writing), no experience requirement, and no renewal requirements. I have advised law students that this certification could be eye catching on a resume given that few attorneys have any credential in cybersecurity. Regarding the CIPT certification, I have started studying for this recently, and it strikes me as very achievable for law students with limited technology background. In this regard, preparation for the test appears to involve reading a 7 chapter book, of roughly 200 pages on technology concepts, and then passing a multiple choice test.

Two legal certifications that are popular in the marketplace (available to both lawyers and nonlawyers) are the IAPP's Certified Information Privacy Professional/US (CIPP/US) and CIPP Europe (CIPP/E). These two certifications focus on US and European privacy law, respectively, with some light coverage of relevant technology principles.

**Part 2: An analogy comparing learning IT to learning Spanish**

Imagine a marketplace where many clients are speaking Spanish, and imagine most legal educators do not speak Spanish. Next, imagine that the number of Spanish speaking clients is expected to continue growing at an exponential rate. Also, imagine significant growth of nonlawyer Spanish speaking

---

40

41 https://www.youtube.com/playlist?list=PLhAOJU2XD-IuR-R6_-8yrENL2glqLEg8s

professionals to meet the growing need.[42] Imagine the opportunities for Spanish speaking lawyers and the necessity for future law students to learn Spanish (of course, by "Spanish" I mean "IT")!

On the surface, a simple solution would seem fairly obvious: teach law students some Spanish! However, while that general goal is simple enough, the execution requires considerable thought.

In the following sections, I explore different language education concepts that could be applied to technology education for law students.

**Fear of speaking foreign languages**

A common fear among human beings is known as xenoglossophobia, a fear of speaking foreign languages.[43] In my own experience, I have observed lawyers exhibit a sort of fear or anxiety when presented with foreign technology terms, and a desire to back away from the tech or to hand off tech issues to someone else. For example, I have heard stories of lawyers asking tech savvy executives to draft portions of contracts involving technology requirements as the lawyers were ignorant on those issues.

Providing students with an education in a subject area, whether in language or in technology, would seem to reduce the fear of the subject.

**Hiring a translator**

In January 2019, Georgetown law school announced that it hired a nonlawyer computer scientist, Professor Matt Blaze, to join its full-time law faculty.[44] According to Professor Paul Ohm, this was the first such hiring of a nonlawyer at any law school in the country.[45] Per this announcement, Professor Blaze "'will teach innovative, interdisciplinary courses at the law school, including Technology of Surveillance and Electronic Voting Technology and Law,' says Ohm."[46]

**Spanish for lawyers courses**

Various law schools provide programming for lawyers courses, with a general focus on learning programming and its application to law.[47] Such courses seem helpful and potentially popular among students. A contrasting idea is to allow students to take introductory programming courses in a computing school and to sit alongside IT students. Both types of courses likely have benefits to law students. On the one hand, a programming for lawyers courses specifically focuses on the programming in the legal industry. On the other hand, a general introductory programming course may benefit law

---

[42] *See,* https://www.bls.gov/ooh/computer-and-information-technology/home.htm ("Employment of computer and information technology occupations is projected to grow 13 percent from 2016 to 2026, faster than the average for all occupations.") (last modified April 12, 2019).

[43] https://en.wikipedia.org/wiki/Foreign_language_anxiety

[44] https://www.law.georgetown.edu/news/one-of-worlds-leading-cryptographers-to-join-georgetown-faculty/?et=editorial&bu=Law.com&cn=20190128&src=EMC-Email&pt=Ahead%20of%20the%20Curve

[45] https://www.law.georgetown.edu/news/one-of-worlds-leading-cryptographers-to-join-georgetown-faculty/?et=editorial&bu=Law.com&cn=20190128&src=EMC-Email&pt=Ahead%20of%20the%20Curve

[46] https://www.law.georgetown.edu/news/one-of-worlds-leading-cryptographers-to-join-georgetown-faculty/?et=editorial&bu=Law.com&cn=20190128&src=EMC-Email&pt=Ahead%20of%20the%20Curve.

[47] *See, e.g., https://law.stanford.edu/education/degrees/joint-degrees-within-stanford-university/law-and-computer-science/* (last visited July 24, 2019).

students by placing them in the same classroom as IT students and might facilitate learning the language of tech from interaction with technology students.[48]

**Spanish Immersion**

"Spanish immersion" could involve law students and faculty attending full day conferences concerning technology issues. This certainly seems common as legal technology issues are hot topics in law schools. Inviting technologists and other nonlawyer IT professionals to such conferences can be a helpful way to improve learning the language of IT.

Another immersion concept might involve placing law students and technology students in the same classroom.[49] This is happening with DePaul's cross listed computing school courses. The Business Continuity/Disaster Recovery course touches on legal issues, such as HIPAA compliance. Students might learn that the Office of Civil Rights imposes hefty fines for any data loss.[50] They also learn the related tech concepts that for a backup data center a "hot site" is preferred over warm or cold sites given that a HIPAA compliant organization needs an RPO of zero (RPO, recovery point objective, essentially means an acceptable amount of data loss, so an RPO of 1 day means an organization can accept up to one day's worth of lost data).[51]

**A semester abroad**

Another learning tool could be a "semester abroad," which would involve a student interning for a lawyer or even a non-lawyer working on tech issues. Certainly, law schools could encourage tech-focused internships at law firms, consulting firms, in-house situations, or even technology firms.

**How much Spanish?**

A hypothetical Spanish curriculum could involve two introductory Spanish courses (e.g., Spanish 101 & 102), followed by two intermediate courses (e.g., Spanish 201, 202), followed by one or more advanced courses. Conceivably, a student who has completed some intermediate coursework may have the ability to not only listen and comprehend but to also respond. Reaching such a threshold could be considered a basic foundation for further learning. In my own experience with IT education, I found that after completing four or five IT courses I was able to have somewhat intelligent conversations with tech executives; I could understand much of what they were describing, and I could respond with a somewhat intelligent comment or question.

---

48

49 Sybille Heinzman *et. al.*, *The Effect of Study Abroad on Intercultural Competence: Results from a Longitudinal Quasi-Experimental Study*, 26 Interdisciplinary J. of Study Abroad 187, 203 (Sept. 1, 2015).

50 *See OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement*, available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html (Feb. 7, 2019).

51 *See generally*, Barry J. Gillin, *Optimizing Recovery of Critical Systems Through Replication to the Cloud*, available at https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/24351/Gillin_2018.pdf?sequence=1&isAllowed=y (2018).

Based on this hypothetical Spanish curriculum, and my own experience taking tech courses as a cybersecurity student, I arrived at an estimated range of 3-6 tech courses as providing students with a basic or low level of tech fluency as a foundation for further learning.

**Required Spanish?**

Some law schools could impose a requirement consistent with Florida and North Carolina's mandatory tech CLE; however, imposing additional rigid curricular requirements may burden schools administratively.

**Include "Spanglish"?**

My third curricular priority is that law schools consider offering interdisciplinary law courses that incluce a blend of law and tech (e.g., perhaps 25% of the law course content embodying tech instruction). Embedding tech instruction in a law course can reinforce concepts learned in IT courses (or supplement them with additional tech concepts). This could be accomplished by law faculty, FT or adjunct, having sufficient tech background to teach tech, or by having law faculty integrate a technologist guest speaker within perhaps 2-3 weeks of a course. Law school leadership would need to encourage faculty to teach and *test* on technology, viewing technology *as a competence* to be tested, just as the legal principles in the course are tested as a competence.[52]

My law course Data Privacy Law: US & EU is an example of an interdisciplinary law course. I launched this course in the spring of 2019, and I included the goal of teaching and testing students on technology as a competence alongside the legal principles. I would estimate that 25-30% of the lecture content constituted tech education. On my spring 2019 final exam, I included a traditional essay involving GDPR issues and approximately 50 questions that were either multiple choice or short answer. Of these 50 questions, about 13 were tech focused. For example, I had a short answer question asking students to very briefly explain what a domain name server and another question asking them to generally describe how a VPN functions (concepts I presented in my lecture videos).

When developing the course, my initial instinct, viewing this as a "law" course, was to keep the course siloed by minimizing tech concepts and focusing mainly on the law. However, two experiences caused me to abandon this traditional siloed mentality. First, in the fall of 2018, I guest lectured twice in a traditional privacy law course, and the professor asked me to focus specifically on tech concepts relevant to privacy. In my guest lectures, I discussed several tech focused cases, including *FTC v. Wyndham*, a case involving an FTC fine for defendant misrepresenting that it had strong cybersecurity controls when in reality it lacked most necessary controls, such as functioning firewalls and encryption of stored data.[53] After discussing the legal concepts, I explored a variety of tech concepts: what firewalls are, how firewall rules function, host based vs. network appliance firewalls, formation of a demilitarized zone (DMZ) with one firewall (i.e., three-legged firewall architecture) versus formation of a DMZ with two firewalls (i.e., placing servers in between two firewalls), local encryption versus public key encryption, and a variety of other tech concepts and legal principles. After my first guest lecture, a British attorney/LLM student

[52] Victoria Hudgins, *States Require Lawyers to Have Tech Competency, but Observers See Some Struggling*, available at https://www.law.com/legaltechnews/2018/10/25/states-require-lawyers-to-have-tech-competency-but-observers-see-some-struggling/?slreturn=20190624173425 (October 25, 2018).
[53] *FTC v. Wyndham*, 799 F.3d 236 (3d Cir. 2015).

approached me to tell me that the lecture was "f---ing awesome" as he was so eager to learn about technology to facilitate his communication with clients. In my nearly 15 years of teaching law school, this was the most exuberant response I have ever experienced after lecturing. Besides this student experience, a second experience that inspired me to make tech education a goal in my law teaching involved meeting with a HIPAA attorney who had over twenty years of practice experience. I described my guest lecturing experience to her and showed her some of my tech focused slides, and she explained to me that she would immediately pay for any CLE that had such content and affirmed that my tech focused approach should be a huge help to serving clients.

**Law schools have limits on how much tech education they can provide**

A law school has a core function of preparing students to pass the bar exam, so a law school cannot become an IT school, and the extent of its tech offerings is therefore limited. Therefore, law school may need to cap the number of JD credits it will allow for a student taking IT courses. Also, law schools may struggle finding law faculty with the requisite technology background to effectively teach technology as a competence within a law course.

That being said, my twofold proposal above of providing JD students with at least three IT electives and offering at least some interdisciplinary law courses seems feasible, and may be a goal that law schools wish to pursue.

**Areas of study**

As noted above, coursework that addresses both networking and programming concepts seems beneficial for law students to get a sense of the OSI layers. However, any variety of tech courses should increase understanding of various OSI layers (e.g., an information security management course). In fact, I could consider digital forensics as another category. Forensics seems to involve both networking and programming concepts as well as system concepts (e.g., Windows Registry keys, deleted files in unallocated memory space, etc.).[54] Forensics is a wonderful area of study for lawyers because it is so integral to both eDiscovery/litigation and incident response.

IT is a fairly broad subject area with many dialects. However, learning one dialect seems effective in terms of quickly understanding another dialect.[55]

As noted in the intro, law students would benefit from some "under-the-hood" instruction as most liberal arts students entering law school lack this awareness. It is a myth that millennials understand technology and do not require tech instruction.[56] . While it's true that millennials have grown up with technology and are likely more adept than prior generations at its usage, this technology usage is typically on the user

---

[54] Gary C. Kessler *et. al.*, *Pedagogy and Overview of a Graduate Program in Digital Investigation Management*, Proceedings of the 41st Annual Hawaii International Conference on System Sciences (Jan. 2008).
[55] *See, e.g.,* J. E. Howland, *It's all in the language: Yet another look at the choice of programming language for teaching computer science*, J. of Computing in Small Colleges 58, available at http://www.cs.trinity.edu/~jhowland/ccsc97/ccsc97/ (1997).
[56] Kari Boyle, Do Lawyers and Law Students Have the Technical Skills to Meet the Needs of Future Legal Jobs?,Slaw (June 29, 2017) at http://www.slaw.ca/2017/06/29/do-lawyers-and-law-students-have-the-technical-skills-to-meet-the-needs-of-future-legal-jobs/

side.[57] Millennials without tech education are unlikely to have any concept of network architecture, public key encryption, or various other under the hood concepts that would be helpful to understand tech with sufficient depth when communicating with clients, courts, or regulators on tech issues. Certainly, any courses involving networking or programming concepts would provide some depth of instruction to better understand the OSI layers as many law students will end up managing in layers 8-10 of Swire's model. For example, many legal scholars have written about the importance of blockchain.[58] Blockchain technology includes substantial networking and programming concepts[59], so law students having education in these areas should be in a better position to understand blockchain (both existing features and new developments) than law students lacking such education. Likewise, many legal scholars have written about AI[60], and any depthful understanding of AI requires a general understanding of programming and networking concepts.[61] While legal scholars tend to focus on the usage of AI and blockchain and the legal implications of their usage, lawyers could benefit from a deeper understanding of how blockchain and AI work from a programming and networking standpoint in order to better communicate with technologists on legal issues (e.g., security by design issues as they may relate to GLBA or HIPAA statutory security regulations).

**Linguistics concepts**

The learning Spanish analogy, while useful, is not a perfect analogy because learning a language is often *largely* a process of word substitution for structures and processes that the student is already familiar with in his own language.

Noam Chomsky analyzed languages in the 1960s when he essentially created the field of linguistics.[62] He observed that all languages have nouns (e.g., structures) and verb phrases.[63] When a student learns a new language, he likely already has a concept of the structures and verbs in his own native tongue, and learning the new language is largely a matter of word substitution.[64] For example, a native English speaker knows how to say "I would like a cup of coffee." He already understands what coffee is and understands commands/requests/verb phrases such as "give me" or "I would like." Therefore, learning how to request a cup of coffee in Spanish is largely word substitution: "Me gustaria un café." Un café is "a coffee" and "me gustaria is I would like."

While IT is replete with foreign terminology (especially acronyms), developing some level of IT fluency involves more than mere word substitution. In this regard, IT fluency requires an understanding of basic structures and processes that are also foreign to the novitiate. For example, while the language student understands the structure/noun of coffee and the process of drinking it, she may not adequately

---

[57] *See* Simon Canick, *Infusing Technology Skills into the Law School Curriculum,* 42 Cap. U. L. Rev. 663 (2014).

[58]

[59] For example, blockchain relies on public key encryption as noted in https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/ (Public key encryption is a topic that I teach and test in my Data Privacy Law course.)

[60]

[61]

[62] *See generally,* https://www.britannica.com/biography/Noam-Chomsky (Last Updated July 19, 2019).

[63]

[64] granted, language learning is not merely word substitution as other syntax issues need to be learned (e.g., word sequence, verb tenses).

understand the basic network structures of switches, routers, web servers, firewall appliances nor the processes of DNS server requests, html requests via an https port, TCP handshake, and cookies within the client server model. Therefore, learning IT involves developing an understanding not only foreign terminology but also of associated foreign structures and processes. Therefore, learning new structures and processes especially requires usage of visual aids (as noted elsewhere), such as network topologies or the like.[65]

**Part 3: Technology Vignettes**

I offer a few technology concepts that relate to the law as a way to illustrate the usefulness and relevance of lawyers and law students pursuing some form of technology education. If a lawyer has some technology foundation, such as via the various models discussed above, this would essentially speed her learning curve when addressing technology issues in practice. As noted above, the more tech background a lawyer has, the better as more tech background affords better and faster comprehension.

**Networking Concepts**

An understanding of networking concepts may be valuable to a lawyer in a variety of scenarios. For example, a lawyer may need to evaluate how a breach occurred either as part of reviewing an expert witness report in a data breach or products liability lawsuit or when working on incident response. Another scenario might involve assessing network security relative to statutory compliance (perhaps using NIST or another cybersecurity framework as an analytical tool).[66] Another scenario may involve advising a small to medium size business regarding cybersecurity, including network security, in light of FTC guidance.[67]

In my data privacy law course, I provide a forty five minute lecture on how the internet works, with a variety of granular technical details involved in the process of powering on a laptop through visiting a remote website, such as the motherboard transferring control to the Windows 10 operating system, logging in the university's network, the university's router or DHCP server dynamically leasing a private IP address to the laptop, use of a domain name server to look up the IP address of the website, and a variety of other details leading up to visiting the website. I was inspired to create this lecture based on discussions with practicing technology attorneys who explained to me that one of their first tasks with a new associate is to educate her about how the internet works. This background knowledge seems essential for discussions with technologists on data breach or other privacy/cybersecurity issues as the internet is the common vehicle through which a data breach occurs.

Many basic networking concepts may arise in data breach or compliance discussions, and I will reference just a few of them. Dynamic Host Configuration Protocol (DHCP), private IP addresses, Network Address Translation (NAT), physical MAC addresses, random ephemeral ports versus port 443 of a remote web server, html, TCP handshake, and DNS poisoning attacks. A student learning about basic networking will likely learn about each of these topics. Starting with Dynamic Host Configuration

---

[65] James B. Levy, *Teaching the Digital Caveman: Rethinking the Use of Classroom Technology in Law School*, 19 Chap. L. Rev. 241 (2016).

[66] https://csrc.nist.gov/glossary/term/demilitarized-zone discusses usage of DMZs (demilitarized zones) for network security, which implicates firewall usage.

[67] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Protocol (DHCP), this is a process where a network leases a temporary IP address to a laptop at the time of logging in (such as logging into classroom Wi-Fi). It's "dynamic" in the sense that a user's laptop will receive a different IP address each time you log into the school's network. A school's network may lease a user's laptop a private IP address. Private IP addresses do not appear on the internet and are only used internally. An example of a private IP address range is 192.168.0.0 through 192.168.255.255. A school's network might therefore assign a user's laptop a private address of 192.168.1.10, or some other address within that range, depending on what's available in the router (or DHCP server's) pool of IP addresses. "Host" in this context means a user's laptop. Configuration has the meaning of setting up, so a user's laptop is configured with the particular IP address at the time of logging in. Protocol has the meaning of a standard. Essentially, a user's laptop and the school's network equipment operate by the same standard (i.e., the DHCP protocol) so that a user's laptop and the school's network understand how to communicate with each other on leasing an IP address to the user's laptop.

The next concept is Network Address Translation (NAT). This is a process where a user laptop's private IP address is translated to a public IP address for purposes of communicating with the outside world. It's common for a network to use a single public IP address for multiple computers. For communications between a user's laptop and a remote website, the user's laptop will essentially open a channel of communication with that outside website (e.g., Amazon.com) and reach out to port 443 of Amazon's web server/website. Port 443 is essentially a communication channel associated with https, encrypted communication. For receipt of data from Amazon's website, a user's laptop provides Amazon's web server with a specific port for receipt of data (called a random ephemeral port).[68] This is important because other laptops connected to a user's school's network are all using the same public IP address. Amazon needs a specific port number to associate with the user's laptop to ensure that it is sending and receiving data from the user's laptop and not someone else's on the user's school's network.

A physical MAC address is assigned to the user's laptop from the manufacturer, and thus, is a number that does not change (unlike a temporarily leased IP address). Some networks track users' physical MAC addresses for security or other purposes.

A TCP handshake is the process of opening a communication "session" between the user's laptop and Amazon's website (i.e., its web server).[69] It is sometimes called a three-way handshake because of how it works. The TCP handshake implicates layer 4 of the OSI model. Without getting technical (we'll leave that to the footnotes), the process works in three general steps:

(1) your laptop asks the Amazon web server "can we talk"?

(2) Amazon responds, "yes we can talk"

(3) your laptop replies, "ok, let's talk"

This three-way handshake is essentially a negotiation between the user's laptop and the remote web server, which involves all necessary information to open the session (e.g., IP addresses, port numbers,

[68] discuss random ephemeral port

[69] *See generally*, Phillip Miller, *TCP/IP Explained* (1997).

etc.) Understanding, the three way handshake/TCP protocol can be helpful to understand how particular cyber attacks may work with respect to TCP vulnerabilities.[70]

Understanding a DNS attack requires an understanding of DNS. DNS stands for Domain Name Service. Essentially, when a user types Amazon.com into her web browser, her laptop asks a domain name server for the IP address of Amazon.com.[71] This is similar to looking up a phone number for Amazon, and it's something her computer does automatically behind the scenes. Her school likely has a domain name server, a computer dedicated solely to the task of providing IP addresses to student and faculty laptops and other computers. In a DNS poisoning attack, that domain name server is compromised by an attacker, such that when her laptop requests the IP address for Amazon.com it is given an IP address for a malicious site instead.[72]

**Firewalls**

Firewalls are one very important component of network security referenced in *FTC v. Wyndham* and are critical for any secure network.[73] Understanding various details of firewalls of how they work would seem helpful when evaluating reasonable security, such as blocking malicious sites, host based vs. network based firewalls, rule order of firewalls, rule exceptions, formation of a demilitarized zone with one firewall (i.e., three legged architecture) versus sandwiching servers between two firewalls. As discussed previously, teaching firewall and other tech concepts is often facilitated by visual aids rather than from words alone as noted by Levy.[74] This seems particularly helpful when assessing a network's architecture and components therewithin.

**Encryption: local vs. data in transit vs. public key encryption**

An understanding of encryption is critical for understanding cybersecurity. Encryption is essentially the conversion of plain text to gibberish so that an eavesdropper cannot easily decipher it. Local encryption applies to stored data and is useful for protecting data stored on a thumb drive or laptop when it is powered off or logged off. Encryption can be used for protecting data or can be used as an attack tool as in a ransomware attack. Encryption complexity is an important concept for understanding the need for sufficient password complexity to withstand a brute force attack.

---

[70] *See* Peter Maynard, Kieran McLaughlin, *Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks*, available at http://www.qub.ac.uk/sites/CSIT/ACEpublications/2016Papers/Filetoupload,734096,en.pdf (2014) ("We only have obscure protocols/systems [ . . . ] if it runs over TCP/IP then it can be susceptible to attacks discussed." Internal quotations omitted.)

[71] *See* Jung Jaeyeon *et. al*., *DNS Performance and the Effectiveness of Caching*, 10 IEEE/ACM Transactions on Networking 589 (Oct. 2002).

[72] *See generally,* Joe Stewart, *DNS Cache Poisoning - The Next Generation*, available at http://ivanlef0u.fr/repo/madchat/reseau/dns/dnscache.pdf (2003).

[73] Other network security tools could include honeypots, intrusion detection systems, intrusion prevention systems, unified threat management tools. etc.

[74] 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 . . . .")

Encryption of data in transit arises in a variety of contexts, such as providing an encrypted email tool for a lawyer's communications with clients, usage of Tor browsers and VPN services (which hide the sender and receiver's identities by encrypting source and destination IP addresses along with the data).

Public key encryption is another important concept that arises in a variety of situations (e.g, Blockchain systems, website certificates, and other digital signatures). In public key encryption, a user is provided with a unique public key that he publishes to the world and also a unique private key that only works with the public key. Generally, if the user, call him Bob, wants others to encrypt communications to him, they may encrypt the messages using Bob's public key. Mathematically, this is a one way function: once the message is encrypted with Bob's public key it cannot be decrypted with that same public key. Essentially, the only way to unlock or decrypt the message is by Bob using his private key. Public key encryption, also known as asymmetric encryption is thus a useful way to inhibit eavesdropping. Another benefit of public key encryption is that it can be used to authenticate a sender of a message, which is relevant to the legal concept of nonrepudiation.[75]

Because of the ubiquity of public key encryption in various IT contexts, an understanding of the basics would seem helpful to technology lawyers.

**Metadata**

Metadata is a very important concept in litigation (civil and criminal) and can have significant legal implications.[76] Metadata is essentially data about a file, such as date created, date modified, author, of GPS data with a photo. It's common knowledge among litigators that a party requesting electronic files in discovery should make sure her requests includes the metadata for that file.

Understanding metadata with photos can be important in various legal contexts. For example, most iPhones automatically include GPS location metadata, indicating the time and precise location that the photo was taken. A lawyer advising a dating website or other site allowing pictures, might advise that the site scrub all metadata from the photos prior to posting them on the site to reduce potential liability; otherwise, a site visitor could easily look up the metadata using standard features in Windows or perhaps using a free iPhone app.

Interestingly, John McAfee, the creator of McAfee Anti-Virus software, was a fugitive many years ago, hiding in South America.[77] He was traveling with a reporter who posted McAfee's picture online without scrubbing the location metadata, allowing authorities to determine his location.[78]

**Hash Values**

An MD5 hash value is essentially a digital fingerprint of either a file or an entire hard drive. Essentially, every file or hard drive is unique in terms of the data stored on it. Therefore, every hard drive produces a

---

[75] https://pdfs.semanticscholar.org/ceda/35b3ac8d680a006dc0aa35fad4321d6227c1.pdf

[76] 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.)

[77] https://www.npr.org/sections/thetwo-way/2012/12/04/166487197/betrayed-by-metadata-john-mcafee-admits-hes-really-in-guatemala

[78] *Id.*

unique MD5 hash value. Just like a human fingerprint, an MD5 hash value of a hard drive produces a value that is distinct from all other computers in the world.[79] Put another way, if one could take an MD5 hash value of every computer in the state of Illinois right now, every computer will have a unique value (in a sense, it is "lottery odds" to have two computers with matching MD5 values).[80]

Another characteristic of MD5 hash values is that small changes in data can produce significant changes in the hash value. For example, if I have two nearly identical 3000 word Microsoft Word files, but they differ by one word, the two files will produce two very different MD5 hash values. For example, I generated an MD5 hash value of a word file of "57146D7D4B33EE6FFF78E1A70AB6BC0F." Next, I changed one word to my fairly long document, and the new value was "11A76A945704BAAE14C751565F933327."

An MD5 value is legally significant because it is a chain of custody tool to show that a forensic image of a party's hard drive or file was not altered during litigation.[81] For example, a plaintiff's forensic expert could make a copy of defendant's hard drive during discovery and save an MD5 hash value at the time of collection. He could then analyze the hard drive looking for evidence relevant to the suit. If the other side alleged that plaintiff or his forensic expert altered the evidence, the plaintiff's side could produce a copy of the forensic image, which would have the same MD5 hash value as at the time of collection, and plaintiff could invite the other side to repeat the same analytical steps on this copy to locate the same evidence.

**Security by design**

Europe's GDPR requires security by design and by default when launching a new IT product or service.[82] U.S. companies seem to likewise be moving in this direction based on GDPR compliance, forward thinking regarding GDPR-like legislation developing in the U.S., and/or as a strategy to reduce exposure. An understanding of computer programming and networking would be helpful for security by design.

With regard to software engineering, "secure by design" means that "...the software has been designed from the foundation to be secure."[83] In a larger sense however, this concept applies to hardware, as well: "Secure by Design principles are pretty straight forward. Security must be considered from system conception, and this focus must continue through all stages of gestation. A system – including all its

---

[79] Yong-Xia Zhao and Ge Zhen, *MD5 Research*, 2010 Second International Conference on Multimedia and Information Technology (Apr. 2010) ("MD5 was developed from MD, MD2, MD3 and MD4. It can compress any length of data into an information digest of 128 bits while this segment message digest often claims to be a digital fingerprint of the data.")

[80] *See, e.g.,* Serdar Osman Onur, *MD5 Hash Collision Probability (Using Birthday Paradox)*, available at http://big.info/2013/04/md5-hash-collision-probability-using.html (Apr. 10, 2013).

[81] Hash values arise in both civil and criminal cases for digital fingerprinting of files. For example, Babcock Power Inc. v. Kapsalis, No. 3:13-CV-717-CRS, 2018 WL 314860, at *1 (W.D. Ky. Jan. 5, 2018) involved an order in a civil case to turn over hash value data during discovery and United States v. Reddick, 900 F.3d 636, 636–37 (5th Cir. 2018), cert. denied, 139 S. Ct. 1617 (2019) involved use of hash values to identify child pornography.

[82] General Data Protection Regulation (GDPR) Art. 25 ("The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are being processed.")

[83] "Secure by design." Wikipedia, retrieved July 24, 2019, from https://en.wikipedia.org/wiki/Secure_by_design.

component parts and their supply chain – must be assumed vulnerable to cyber attack, and developers must build in appropriate defences & warnings."[84]

**Tech topics list**

As a final note, I provide some specific tech topics to consider for teaching data privacy/cybersecurity law.

In my spring 2019 Data Privacy Law: US & EU course, I taught and tested students on various, specific tech concepts, which I viewed as highly relevant to data privacy. I briefly list most of them with the thought that others teaching data privacy could consider embedding these tech topics into their courses: how the internet works (http vs https, ports, client-server model, network address translation, IP addressing, 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, 1st party vs. 3rd parties); IAAS, PAAS, SAAS; VPNs; and DNS.

I am working with a colleague (Prof. Karen Heart, an attorney and computer programmer at DePaul's computing school) on development of a cybersecurity law course (anticipated spring 2020). In this course, we plan on addressing a variety of digital forensics issues (e.g., metadata, hash values, deleted data) and security by design (software and hardware considerations).

**CONCLUSION**

As noted above, I propose that

(1) law students may benefit from under the hood technology instruction in addition to (or rather than solely) user side tech education;
(2) law schools consider three curricular priorities for educating students on tech to meet the demands of 21st Century law practice: (a) provide instruction on networking and programming fundamentals with an emphasis on cybersecurity; (b) provide additional tech coursework in other categories of tech; (c) encourage development of interdisciplinary law courses having a substantial tech component; and (d) teach and test law students on tech as an area of competence; and finally
(3) law schools can consider a foreign language learning analogy when developing a technology curriculum with the goal of helping law students to achieve an intermediate level of tech fluency as a foundation for further learning outside of law school.

[84] Palfreyman, J. "Secure Design," IBM Government Industry Blog, retrieved on July 24, 2019, from https://www.ibm.com/blogs/insights-on-business/government/secure-by-design/.