The Future of Security and Privacy Education: Incorporating Cybersecurity Law and Policy into Cybersecurity Curricula

Paula S. deWitte, J.D., Ph.D., P.E.
Assistant Director, Texas A&M Cybersecurity Center and
Associate Professor of Practice, Computer Science and Engineering Department,
College of Engineering, Texas A&M University
Paula.dewitte@tamu.edu

What new approaches are required in educating the next generation cybersecurity workforce? (1) We cannot educate and train the large numbers of cybersecurity workers required in the United States. The question becomes: *How do we increase the efficacy of those we do educate and train?* (2) We have relative smaller numbers of women and other underrepresented groups in cybersecurity: Similarly, the question becomes: *How do we increase opportunities?*

The Issues: It is unarguable that the evolution of law and policy lags technology development. Both poorly anticipate what *may* occur; rather, society implements new laws and policies in reaction to events. Before the disclosures by Facebook and Cambridge Analytica, most analysts did not expect additional privacy regulations in the United States now being considered. Another issue is a current case before the Supreme Court of the United States (SCOTUS), Carpenter v United States.[1] The long standing legal precedent is that law enforcement does not require a Fourth Amendment Search Warrant to obtain data shared with a third party such as phone logs (i.e., numbers called, time called, call duration, and locations of the parties) with a vendor (i.e., the mobile phone service provider). The SCOTUS decision, due early summer 2018, may require such search warrants based on arguments that the pervasiveness of technology such as smartphones has fundamentally changed the power of technology to be more invasive in areas that individuals have a "reasonable expectation of privacy." Both issues, although seemingly incongruent, are concerned with privacy and protecting individuals when sharing data, either through "apps" or the government. These issues require cybersecurity workers to be cognizant when new legal and policy rules apply.

[1] https://www.oyez.org/cases/2017/16-402

Nor is this confined to domestic law and policy. Cyberworkers need to be cognizant of evolving privacy frameworks such as the General Data Protection Regulation (GDPR) with, among other issues, extra-territorial jurisdiction, broadly defined personal data of "data subjects," and the recognition that many non-EU countries are implementing GDPR (e.g., Singapore, Mexico, Canada).

Students studying cybersecurity today will be the front-line for protection, detection, and response to cyber attacks. They will make decisions within constrained time periods; yet, they are being educated without substantial knowledge of either American or international law and policy. These cyberworkers will not have the luxury of contacting legal counsel for advice because of the sheer volume of decisions and the need for rapid action. What is required is academic curricula devoted to cybersecurity law and policy to develop students' capabilities to analyze and confidently apply emerging laws and policies without constant reference to legal advice.

Such courses are often mis-labeled as "soft skills" and treated as an after-thought rather than an integrated component of cybersecurity curricula necessary to support technical decision-making. Educating front-line protectors, defenders, and responders through tailored course content and pedogeological processes improve the efficacy of cybersecurity workers. This is a better approach than educating more cyber savvy attorneys. [Good luck with that!] This is misguided. It creates yet another legal specialty within the already burdensome, time-consuming legal process, and does nothing to address cyberworkers time-dependent performance requirements.

As students, legal savvy cyberworkers should:

1. Acquire the common body of knowledge for cybersecurity law and policy to include terminology, concepts, and specific legal terminology.
2. Acquire the common body of knowledge related to national and international laws related to cybersecurity and their differences.
3. Apply legal concepts in issues related to cybersecurity including cases/controversies unique to cybersecurity.

4. Identify and explain common legal issues related to cybersecurity.
5. Understand and explain procedural legal requirements relevant to cybersecurity.
6. Demonstrate the ability to use legal and policy knowledge by analyzing cybersecurity issues from a cyber worker perspective such as whether a security incident violates a privacy principle or legal requirement necessary for a valid response.
7. Demonstrate the ability to work through a case study identifying legal issues, analyzing the cybersecurity action required, and formulating a plan that complies with applicable laws.
8. Synthesize an action plan through analyzing cybersecurity legal and policy knowledge issues

Scope of the Issue and Analysis of the NIST NICE Framework: A search on the NIST NICE Framework using search terms of "legal;" "law;" "privacy;" "counsel;" "regulation;" "compliance'" "policy/policies" (an ambiguous term and used only in the context of government policies) "contract," "legislation," or "Executive Order," reveals a number of required tasks and KSAs throughout the seven Specialty Area Categories.

The initial analysis of the Framework found 72 tasks, 26 knowledge IDs, 6 skills, and 12 abilities that require some form of specific law and privacy knowledge. Although cursory , the analysis anecdotally identifies a surprisingly significant number of specialty areas requiring relevant KSAs for non-attorney work roles such as: (1) System Architecture (ARC): *"Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes." or* (2) Threat Analysis (TWA): "*Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities*."

Yet, only two work roles within the Specialty Area "Advice and Advocacy (LGA)" require a Juris Doctorate degree. The LGA specialty: "*Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.*

Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings." The LGA specialty occurs in two work roles: (1) Cyber Legal Advisor (OV-LGA-001) who "*Provides legal advice and recommendations on relevant topics related to cyber law*; and, (2) Privacy Officer/Privacy Compliance Manager (OV-LGA-0021) who "*Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams*."

By comparison, many more work roles with their specialty areas require legal/policy knowledge such as: (1) "*Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy*." [K003]; (2) "*Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).*" [K0044]; or (3) "*Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations."* [K0107].

Workshop: We propose incorporating into the NACE Workshop a discussion on deriving the requirements for courses to address this substantial gap. The proposer taught the first-ever course at Texas A&M University in Spring 2018 addressing the need for legal savvy cybersecurity students. She proposes to offer that syllabus as a point of departure for the discussion. The workshop and its anticipated contribution to curricula development is essential to building analytical capabilities of future cyberworkers to operate within the dynamic and time constrained cybersecurity threat environment.

Additional Benefits: Developing these curricula may help to broaden the spectrum of applicable jobs and may increase the diversity of cybersecurity workforce. In addition to attracting those with engineering and IT skills, expanding the curriculum to develop legal and policy skills may attract students with different analytic and communication strengths, and as a result, both increase their number while improving the competency of the holistic workforce.

.

Paula S. deWitte, J.D., Ph.D., P.E.

Paula S. deWitte, J.D., Ph.D,. P.E., is both a Ph.D. in Computer Science and a licensed attorney in the State of Texas. She is a registered patent attorney with the United States Patent and Trademark Office (USPTO). She is one of less than 100 licensed Professional Engineers in the State of Texas in Software Engineering (SWE). She holds a Bachelors and Masters from Purdue University where in 2015 she was honored as the Distinguished Alumna in the Department of Mathematics, School of Science. She obtained her Ph.D. in Computer Science from Texas A&M University in 1989. She currently is the Assistant Director of the Texas A&M Cybersecurity Center and an Associate Professor of Practice in Computer Science and Engineering. Prior to joining Texas A&M University, she started several technology businesses. She most recently started two companies in oil and gas on a patented process in analyzing drilling fluids [US Patent US 8812236 B1] and has a patent pending through the European Patent Office (currently on review by USPTO) on incident response to a cybersecurity attack in the industrial control environment. She has mentored start-ups at Rice University OwlSpark and the University of Houston RedLabs. Before she joined Texas A&M University in July 2017, she was an Adjunct Professor at the University of Houston.