Deputizing Software Professionals: One case for settling the lawless Digital Wild West in the Golden State

By Rafa Baca, Esq.*

Contents:



## 1. ABSTRACT

Data and computer scientists often encounter great difficulties when their professional work is applied within national legal systems, other than common and civil law systems, that do not guarantee human rights protections to its citizens. Further concerns might arise as current employers may require some professional activity that is either questionably legal or clearly legal but may be objectionable as being personally immoral.

Software professionals are on the frontlines when it comes to developing new online applications for consumers all over the world where regulatory officiating by lawyers, especially in terms of data privacy and digital ethics, invariably occurs after the software has been extensively developed. This paper suggests extending existing State of California professional licensure protocols to further include formally educated software professionals so as achieve higher levels of privacy awareness and digital ethics at the very start of the software development process. Along with lawyers, California licensed software professionals will bring much needed data privacy legal and ethical policy implementation and thus giving rise to the notion of Wild West-syle deputizing of individuals to assist with cyber law enforcement. As Northern California is the principle hub to world's software development industry, a state licensure regime targeted for software professionals that adheres to the highest ethical and technical standards imposed by regulatory legislation ensures, policywise, that the general public and their data is safe within legislatively designated online software platforms and the industry at large.

## 2. PROLOGUE – THE LAWLESS DIGITAL WILD WEST

As technology within the digital domain continues to rapidly expand and affect our everyday lives, building resonate and inspirational communities on Internet frontier is arguably one of the most noteworthy efforts in recent human history. By its very nature, creation is a messy process where a sense of wonder,

lawlessness, amusement, love, and anger can all be seen all at once during this Internet "Wild West" period.

Presently, many communities across the Internet are struggling for a shared moral, ethical, and legal ethos for a fair, consensus of agreeable conduct that can be reliably enforced – a search for an innate digital sense of right and wrong. All online communities tend to agree that there should be baseline understanding of respect and accountability, although there are many approaches for how this understanding should enforced.

Illustratively, groups of entities, namely individuals, corporations, and nations, have recently charted quite different paths toward this unified goal for cyberspace. In many instances, online communities of individuals develop guidelines for conduct within their corresponding fields of interest. For example, in making a small, solitary pledge at Softwarethics.org,[1] individuals working within their professional occupations are in the process of actively developing codes of ethics for software and social engineering on the Internet. Other individuals are compelled toward online activism and even vigilantism to address many digital and physical world objectives, through the actions of such groups as Anonymous; Never Again's "Tech Pledge"[2] and with social engineering certification training programs for hackers.[3]

With the absence conduct in the digital realm that consistently advocates respect for basic human liberties as well as the peaceful, well-being of citizens in other nations, tech companies across the globe are taking a collective initiative toward creating online communities for promoting fundamental online norms while addressing a variety of issues.

## 3. ONE LEGAL CASE FOR ENFORCMENT OF DIGITAL ETHICS THROUGH CALIFORNIA'S CCPA

As professional, individual, and business communities take positive steps to apply codes of digital ethical conduct or become signatories to online petitions, such ethical actions may not be entirely enforceable under the vast, expansive skies and natural landscapes of the lawless Digital Wild West. One must fundamentally realize that justice or fairness is a subset of the concept of ethics and not the law. Specifically, a "just" decision is a fair decision to the extent that each individual within a community is treated equally in terms of what they need or deserve.[4] In other words, justice is a principle by which "we render to each what is due and treat like cases alike."[5] Modern democratic legislatures, the courts although to a lesser extent, and similar governing bodies decide what emergent ethical principles, including principles of justice, should be transformed to written law.[6]

Illustratively, the European Union (EU)'s General Data Protection Regulation (GDPR)[7] is one recent and notable transformation of digital ethics to written law to combat recurring digital data breeches by corporations through ensuring commercial regulatory compliance. The GDPR serves as an exemplary roadmap for privacy and protection of EU citizens' personal data. Leveraging on the European Union's fundamental right to data privacy,[8] much of the GDPR enforces a notion of personal privacy by default where users must opt-in to be tracked by the accessed

software. Notably, the GDPR provides regulations requiring a data breaching company's designated Data Protection Officer[9] to promptly report a data breach directly to the EU Member State's, for example Spain or Germany, designated GDPR Supervisory Authority.

Recognizing that in the United States privacy is not a fundamental civil liberty as in the EU, the U.S. State of California used the GDPR as the primary template for enacting the California Consumer Privacy Act of 2018 (CCPA)[10] that enables California consumers to be aware as to how their electronic data is managed by software companies and the right to opt-out of corporate accounting of personal data. Contrastingly, the CCPA does not provide for a role of a Data Protection Officer as the GDPR, although the CCPA permits strong deterrent remedies against a would-be data breach. For example, the CCPA provides for individual or a class action of consumers to additionally recover statutory damages if the breaching data company failed to implement a reasonable data security assessment and plan.[11]

## 4. ANOTHER CASE FOR ENFORCMENT OF DIGITAL ETHICS GIVEN LEGAL PRESCEDENCE WITH LICENSING AND MAINTAINGING STATE LICENSES TO PROFESSIONAL ENGINEERS

The legal concept of professional engineering licensure in the United States first came about in Wyoming in 1907 as non-engineers, such as lawyers and notaries, were making poor quality technical bids to the State of Wyoming for access to water.[12] Today, unlike the fact that all practicing lawyers must be licensed by a state bar, state licensed, registered or "professional" engineers, "P.E's", is an optional process administered by each state board where refraining from this P.E. exam process does not prohibit engineering graduates from working within their chosen field. Generally, professional licensure for engineers is a two-step process:[13] first "bar exam" like test or tests that includes an engineering ethics component graded by the licensing state must be successfully passed. The second step requires that a professional engineer candidate to accumulate a few years of engineering work experience as an Engineer in Training (EIT). Similar to maintaining state law licensure, the majority of U.S. states require an accumulation of combination of continuing education and professional development credits for licensure compliance and renewal for professional engineers[14] in a manner similar to maintaining lawyers' MCLE requirements for annual bar renewals.

For formally trained computer and data scientists, software engineers, and information technologists state professional licensures similar to that of engineers presently do not exist. Arguably, these "software professionals" can receive certifications of varying competency from various commercial vendors such as Microsoft[15] and Oracle but these commercial certifications lack legislative input that both promotes and embeds public policy, ethics and other non-commercial standards that benefit the greater public welfare, including personal privacy, as requirements for licensure. Although tech companies have made efforts to collectively impart ethical training to software professionals, these corporate efforts often lack enforcement of accountability that includes traditional civil and criminal penalties by law enforcement of various governing bodies. Today's continuing

media saga of tech CEOs appearing and yet reappearing before U.S. Congressional oversight hearings regarding digital privacy provides ample evidence of the existing lack of viable enforcement of ethical and legal principles to where lawmakers are not entirely satisfied with state of digital privacy at this time but are confounded as to finding a viable way of regulating digital privacy.

Like engineers, software professional are highly trained technical professionals that are coveted by employers everywhere. Both of these groups of technical professions take pride in their hard work and sincerely want their work product to better daily lives of their community. In practice, software professionals are not always mindful of the legal regulations and ethical conduct that should be adhered to during software development or with what is being required by their employers in terms of digital rights and privacy concerns. Often the task at hand for software professionals involves successfully building-out "use cases" in an iterative, and highly rapid manner that, in practice, is rarely conducive to oversight by legal departments during development.

## 5. THE LEGAL AFFECTS OF AN OPTIONALLY LICENSED SOFTWARE PROFESSIONAL

Possibly, for the State of California to legislate professional licensure of software professionals and overseen by a state licensing board, yields at least two general benefits to a licensed software professional, they are: (1) highly likely that a licensed software professional would enjoy nearly the same benefits as a professional engineer under the California Professional Engineers Act ("the Act")[16] and supporting Board Rules;[17] and (2), possibly, licensed software professionals would be granted the extra legislative authority of a Data Protection Officer similar to the EU's GDPR but lacking in California's current effective version of the CCPA.

### a. FORSEEN BENEFITS AS WITH PROFESSIONAL ENGINEERS & RESPONSIBE CHARGE

Many professional engineering organizations have elaborated on the benefits of professional engineering licensure at this time. Because engineers and software professionals are both highly technical career fields that require formal education, it is likely that licensed software professionals would enjoy nearly the same the benefits as professional engineers do today. Accordingly, the two most commonly noted benefits are that licensed professional engineers get about 5% more pay than other engineers and that professional engineers are highly esteemed by their engineering colleagues.[18] The job market typically pays more for professional engineers as their optional accomplishment of successfully navigating an arduous licensure process as well as maintaining a continued professional education, including ethics, demonstrates a bright and highly motivated professional that would make an ideal employee and leader that is always heavily sought out in the marketplace.

Exclusive job opportunities are provided to certain professional engineers. A licensed engineer can readily enjoy private consulting work, including exclusive projects that require an engineer to "sign-off" and affix a "seal" on a project, namely

the legal concept of "Responsible Charge".[19] Accordingly, in terms of state legislatures and other governing bodies, large municipal projects that use public money require engineering plans to be designed and executed toward providing a benefit to the greater public. As such, state legislatures and other governing bodies look to professionally licensed engineers to act on each municipal project with the utmost care and applying the highest possible standards. Specifically, the ongoing governmental policy directives implemented by licensed professional engineers are meant to apply higher standards of ethical care, quality, and specialized technical skills toward a specially designated project that is widely and safely accessed by general public, such as bridges, airports, and high-rise elevators for example.

One example, widely known to the general public, often highlights the activities of civil engineers. In particular, only professional civil engineers can sign-off on the formal engineering plans for a bridge or other public works project before starting. Certain governmental engineering project opportunities will only be granted so long as a licensed civil engineer or other professional engineer assumes signature or responsible charge on such work.

On the other hand, it must also be noted that the benefits associated with responsible charge may also detrimentally incur legal liability,[20] by design, for instances where a licensed professional engineers act in an illegal or unethical manner. Similarly, lawyers who carry professional liability or malpractice insurance are well aware of the privilege and power of signing-off on a client's court document bears the added responsibility to act ethically and legally with all transactions. As professional engineers' and lawyers' livelihoods rely on best and ethical practices, liability remains a practical means for strictly promoting ethically favorable behaviors within those professions. Furthermore, professional insurance carriers that underwrite lawyers and professional engineers actively engage with licensed practitioners to promote and educate behaviors that avoid professional malpractice liabilities as part of their insurance underwriting services as well.

b. AUTHORITY TO PROVIDE OBJECTIVE 3rd PARTY DATA SECURITY ASSESMENT CONSULTATIONS

As yet another possible component to the state of California endowing responsible charge upon licensed software professionals, exam material and professional coursework might further foster the ability to conduct and sign-off on third party Data Security Assessments as currently required by the CCPA. To avoid court class-action lawsuits under the CCPA by mitigating or eliminating trial pleadings for statutory damages, licensed software professionals can play an active role in implementing and maintaining a comprehensive information security programs as a third party consultant.[21]

Interestingly, on a federal level, the U.S. Federal Trade Commission (FTC) in its 2019 Privacy and Data Security Update challenged businesses to review whether their actual data practices align with user expectations and online public facing terms and conditions statements in a manner very similar to the CCPA's encouragement of maintaining comprehensive security programs.[22] Accordingly, if such California legislation proposed by this paper is implemented, it would be helpful to have the FTC provide comments to potential California legislation to

strengthen in impact and activity of licensed software professional in the context of licensure further providing authority of implementing and maintaining a comprehensive information security programs. This notion would indeed provide greater incentive toward becoming a licensed software professional.

## 6. A CASE FOR DEPUTIZING SOFTWARE PROFESSOINALS

Arguably, as the 21st century Internet infrastructure as often compared a public utility, such as municipal electric and water systems, there exists a government policy interest to ensure the general public and their data is safe in a variety of online or other type of digital circumstances. Illustratively, in terms of data privacy, there is a small patchwork of existing federal and state laws that, in policy, protect data privacy in only some commercial industries, such as with healthcare and financial data. Moreover, this disparate patchwork of laws is typically enforced by a handful of federal agencies with narrow jurisdiction and limited means for full recourse, such as the U.S. Federal Trade Commissions enforcement of online advertising and privacy of financial data[23] as well as the U.S. Department of Health & Human Service's Office of Civil rights for enforcing health data privacy.[24]

Within most tech companies, legal departments presently assume much of the burden of ensuring implementation of such data and privacy laws and policy. In practice, most all lawyers have no formal technical education so as to effectively communicate and educate data policy restrictions and laws directly to software professionals on their own highly technical terms that includes highly specialized terms and vastly different work culture to that of lawyers. Oftentimes, communicating legal concepts to software professionals is but one of a myriad of other roles that lawyers engage on the behalf of a typical software company at any given time. As evidenced by a large number of online massive security breaches and policy mishaps demonstrated in the daily news regarding tech companies, the current channels of communication and implementation of legal and regulatory policy between the legal departments and software teams needs improvement beyond today's methods.

Effectively, as strong argument can be made that deputizing software professionals to be mindful and help enforce data privacy laws within their environment where software products are first created and perfected. The idea of deputizing software professionals to become legal vanguards that work along with existing legal departments to provide greater assurances to the general public that their data is safe within certain online software platforms. Specifically, reminiscent of Old Western lore, one way of deputizing software professionals to become legal assistants or, alternatively, practice within a highly narrow field of law. Like the field of engineering today, granting optional licenses to software professionals of the highest technical and ethical standards will come with financial and reputational rewards as well possibly acting under a new legal role.

Moreover, extending this notion further, there is even long-standing, successful prescient for non-lawyer, highly-technical professionals to practice law that specifically lies within the exception granted by act of U.S. Congress for a highly

technical and narrow situation where U.S. Patent Agents work on patent matters before the U.S. Patent and Trademark Office (USPTO).[25] Similar to what this paper proposes, qualified engineers and scientists pass a licensure exam provided by the USPTO to practice administrative legal matters regarding patents within the federal agency, the USPTO. To this end, strictly within this narrow scope of patent matters, patent agents must abide a code of ethics as well as by patent agent client confidentiality and privilege in the same manner as attorney client confidentiality and privilege.[26] Accordingly, as proposed in this paper, there is prescient to afford limited legal capacity to highly technical non-lawyer individuals so as to deputize software professionals to help implement and enforce data privacy laws under the CCPA as software is being created and not after the fact which is often the current domain applied exclusively to lawyers today.

At this time, where it is both incohesive and well-lobbied by disparate special interests, the U.S. Congress is effectively far from adopting a Digital Bill of Rights or Amending the U.S. Constitution to bestow a right of privacy to all citizens as what the current Constitution of the European Union provides. Although this present notion of establishing a state license for software professionals falls short of endowing each U.S. citizen with a constitutional right to privacy, including digital privacy, such California state legislation proposed by this paper provides a direct, quick, and effective way to change the norms of an entire industry with continuous regulatory enforcement of some actions performed by licensed software professional to benefit the data privacy rights of the general public. First, along the lines of proposed state legislation, California should enact laws that provide for optional professional licenses for software professionals along with establishing an overseeing state licensure board. Secondly, to further persuade software professionals who obtain an optional state license, California should amend the existing CCPA to include provisions to include licensed software professionals to become Data Privacy Officers under the CCPA, similar to the GDPR, as well as possibly non-lawyer legal professionals, under highly narrow circumstances, under the California law.

## 7. EPILOGUE – BRINGING LAW & ORDER TO THE DIGITAL WILD WEST

One often hears the popular adage, “So California goes, so goes the nation”. Given that the Santa Clara Valley of Northern California, i.e. “Silicon Valley”, is the software capital for the world at this time, therefore so as California legislatively moves to provide optional licensure to software professionals, then so will the nation as well as the world as most software companies headquartered or with research and development in Silicon Valley would need to comply with California law in the due course of business. In this manner, the marketplace would financially reward these software professionals who adhere to a stricter level of technical as well as ethical competence to ensure the general public and their digital data is safe as a matter of public policy. As much of the world’s software corporate headquarters and technical talent resides in California, enacting state legislation for optional licensing would ensure continuous training of licensed software professionals on ethical policy determined by the state. Therefore in practice,

California, and not the U.S. Congress, would be at the vanguard of establishing digital privacy ethical norms, regulations, and laws to the entire global software industry, beginning with administering the initial board exams as well as regulating professionally accredited coursework on licensure renewal for software professionals.

* Rafael "Rafa" Baca, is a practicing U.S. Patent Attorney and Software Developer with a Masters in Computer & Data Science, and Bachelors in Mechanical Engineering. Rafa is a Chair of the American Bar Association Artificial Intelligence Committee and is an active Silicon Valley Entrepreneur, TV Host, Angel Investor, Texas Wildcatter, Photographer, Scuba Diver, and aspiring Chef.

FOOTNOTES:

1. Software Professional Code of Ethics. SoftwareEthics.org. http://www.softwareethics.org/

2. Our pledge. neveragain.tech. http://neveragain.tech/

3. Learn Social Engineering from Scratch: Learn how to hack accounts and personal devices & and how to secure yourself from hackers. Udemy.com/course/learn-social-engineering-from-scratch. https://www.udemy.com/course/learn-social-engineering-from-scratch/

4. *Morality, Ethics, and Law: Introductory Concepts*, Jennifer Horner, Ph.D., J.D., Seminars in Speech and Language, Vol. 24, No. 4, pp. 263 -274 (2003); p. 267.

5. Id. at p. 268.

6. *Law Morals & Ethics*, Geoffrey C. Hazard, Jr., Yale Law School, 19 S. Ill. L. U. L. J. 447-458 (1994-1995); at p. 456.

7. (GDPR) – Regulations (EU) 2016/672.

8. Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389, Article 8 Right to Protection of Personal Data.

9. Id. at Art. 37-39.

10. Cal. Civ. Code §1798.100 *et seq*. (California Consumer Privacy Act of 2018). Title 1.81.5 Ch. 5, Sec. 3 California Consumer Privacy Act of 2018

Sec. 1798.100 *et seq*.
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.100.&lawCode=CIV

11. Cal. Civ. Code §1798.50.

12. From humble beginnings in a Western outpost, licensed professional engineers have spent the past 100 years building a reputation for competence, integrity, and service in the public interest. Doug McGuiry, The Magazine For Professional Engineers, pp 25-29 (June 2007) National Society of Professional Engineers. https://www.nspe.org/sites/default/files/resources/pdfs/pemagazine/june2007_the_professional_engineering.pdf

13. *See* What is a PE? https://www.nspe.org/resources/licensure/what-pe

14. The Benefits of Earning and Maintaining a Professional Engineer License. InnovationAtWork.ieee.org https://innovationatwork.ieee.org/the-benefits-of-earning-and-maintaining-a-professional-engineer-license/

15. Browse Role-based Certifications. Microsoft.com/en-us/learning. https://www.microsoft.com/en-us/learning/browse-all-certifications.aspx

16. Professional Engineers Act (Business and Professions Code §§ 6700-6799), Cal. Bus. & Prof. Code, §§6700 *et seq*.

17. Title 16, California Code of Regulations §§ 407- 476 (Board Rules under the Professional Engineers Act), 16 CRR §§400-476.

18. *See generally*, The Benefits of Earning and Maintaining a Professional Engineer License. Id.

19. Cal. Bus. & Prof. Code, §6703; 16 CCR §404.1; see also BPELS Enforcement Unit Staff, Guide To Engineering and Land Surveying for City and County Officials. (California Board for Professional Engineers and Land Surveyors 2019) pp 6, 24. https://assets.jsheld.com/uploads/Practice-Guide-for-California.pdf?mtime=20190708202135

20. *See* generally Cal. Statutes 2010, Ch. 698; Cal Code Civ Proc §§ 996.310-996.360; Bus. & Prof. Code, §7071.6.5 (business entities of licensed professionals are required to obtain a surety bond, insurance).

21. Cal. Civ. Code §1798.150.

22. FED. TRADE COMM'N, 2019, PRIVACY AND DATA SECURITY UPDATE, at p12 ("Advocacy").

23. Id.

24. HIPAA Enforcement. hhs.gov/hipaa. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

25. *In re Queen's Univ. at Kingston,* No. 2015-145, at p. 23 (Fed. Cir. Mar. 7, 2016). https://foiadocuments.uspto.gov/federal/15-145_1.pdf

26. Id.