



# The State Bar of California

## **Consulting Group on the Establishment of a Legal Specialization in Privacy Law**

### **Report and Recommendations**

## EXECUTIVE SUMMARY

In September 2021, the California Lawyer’s Association (CLA) submitted a letter and proposed a new specialty area application for Privacy Law. The California Board of Legal Specialization (CBLS) adopted the following recommendation: (1) that a State Bar privacy law specialization be further explored; and (2) that staff begin work on a proposal to the Board of Trustees for creation of a Privacy Law Consulting Group. At its December 17, 2021 meeting, the CBLS reviewed and approved the request to delegate authority to the CBLS Chair to appoint the new specialty area consulting group consisting of a working group of 11 attorneys and two public members. Staff worked with the CBLS Chair to appoint members to the working group. They were charged with evaluating whether the CBLS should adopt Privacy Law as a specialty area. The Consulting Group on the Establishment of a Legal Specialization in Privacy Law (PLG)’s exploration unveiled the need to address the ever-growing importance of privacy concerns and the increasing complexity of data-protection regulations.

In recent years, the landscape of data privacy has evolved significantly due to rapid technological advancements and the widespread use of personal data. Individuals, businesses, and organizations face a myriad of challenges concerning data protection, cybersecurity, and compliance with an array of privacy laws and regulations. To meet the demands of the legal professionals who specialize in data privacy, the California Lawyers Association (CLA) established a Privacy Law Section in November 2020. Its membership grew from 0 to 900 within months of its establishment and it now has over 1,200 members. The Section provides a vast array of education events and programming that members consume and interact with, including the Inaugural Annual Privacy Summit which took place in Los Angeles in February 2023 with over 200 attendees. As an indicator of the market and industry need, the CLA Privacy Law Section’s LinkedIn and other social media channels following grew from 0 to 1,500 since they were launched.

As the state of California continues to lead in consumer privacy protection with the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), it is vital to have qualified legal professionals capable of navigating and interpreting these complex regulations. The California State Bar’s Legal Specialization Program’s intent is to provide a method for attorneys to earn the designation of certified specialist in particular areas of law, increasing public protection and encouraging attorney competence. By establishing a specialty area, specialists will express expert-level competence that will help address the increasing needs of consumers and address the gap that currently exists in this field.

## BACKGROUND

The California Board of Legal Specialization (CBLS) is a distinguished regulatory body established to uphold and promote the highest standards of legal expertise and professionalism within the state's legal community. Operating under the umbrella of the State Bar of California, the CBLS plays a pivotal role in recognizing attorneys who have demonstrated exceptional competence in

specialized areas of law, thereby enhancing the quality of legal representation and safeguarding the interests of clients.

Founded with the mission of fostering legal excellence and protecting the public interest, the CBLS offers an array of certification programs that allow attorneys to showcase their specialized skills and knowledge in diverse practice areas. Through a stringent and transparent evaluation process, the CBLS ensures that certified specialists possess a comprehensive understanding of their respective fields, equipping them to provide exceptional counsel and representation to clients facing intricate legal challenges.

Embracing a commitment to professional development, the CBLS actively encourages attorneys to pursue continuous education, engage in scholarly activities, and remain updated with the latest legal developments in their specialized areas. By facilitating ongoing learning and engagement, the CBLS ensures that certified specialists remain at the forefront of legal knowledge, thereby elevating the overall standard of legal practice in California.

In line with its dedication to promoting the welfare of the public, the CBLS serves as a reliable resource for individuals seeking competent legal representation. By referring clients to certified specialists, the CBLS aids in fostering a trusting relationship between attorneys and their clients, enhancing transparency, and facilitating informed decisions in legal matters.

As an esteemed authority in the legal community, the CBLS continues to be an instrumental force in shaping the legal landscape of the state. Its commitment to recognizing exceptional legal proficiency, promoting ethical conduct, and ensuring public trust reinforces its status as a cornerstone of excellence within the legal profession.

Two applications were submitted for interest with the CBLS in Privacy Law; one in 2019 by the International Association of Privacy Professionals (IAPP) for accreditation of a specialty certification program and the other in 2021 by the California Lawyers Association (CLA) for a proposed new specialty area. Both organizations discussed the need and the interest in Privacy Law Specialization. In response to the CLA specialty application, this consulting group has been created.

## **HISTORY OF PRIVACY LAW IN CALIFORNIA**

Privacy law in California has evolved rapidly over recent years and privacy is now of critical importance to the public. Technical advancements and more malicious internet usage have dramatically changed the privacy risks that individuals face today due to the continuing growth of big data, and governments wrestle with how to best protect individuals through the implementation of an overlapping patchwork of statutes and regulations. The need for attorneys with privacy expertise has never been greater and will continue to expand at a rapid rate.

Privacy Law as a field had a slow beginning with a relatively narrow scope in comparison to other fields. Privacy in the United States can be traced back to the passage of the Bill of Rights amending the U.S. Constitution in 1791 with the Third, Fourth, and Fifth Amendments. The amendments grant freedom from the quartering of soldiers as a safeguard against government intrusion into personal affairs, as outlined in the Third Amendment. Additionally, the Fourth Amendment guarantees protection from unreasonable searches and seizures without probable cause, serving as evidence of the right to privacy in an individual's body, homes, and papers. Furthermore, the Fifth Amendment has been interpreted to justify the protection of private information by safeguarding against self-incrimination. Such interpretations have led to the conclusion that there is a Federally-protected right to privacy. While the Amendments were aimed at protecting individuals from government intrusion, more recent privacy laws have created protections from private entities. In 1914 the Federal Trade Commission was established, and in 1917 Judge William Lamar ruled against the Bureau of Investigations' ability to open and read private mail for purposes of investigating acts of foreign sabotage. A few decades later in December of 1948, recognition of privacy rights began to gain momentum when the United Nations recognized the right to privacy in the Declaration of Human Rights, stating that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Privacy in the United States then gained traction with *Griswold v. Connecticut* in 1965 where the Supreme Court recognized the "right to marital privacy", then in *Katz v. United States* in 1967 where the Fourth Amendment protections against unreasonable searches and seizures were applied to where a person has a reasonable expectation of privacy, and in the same year, in 1967, California enacted the Lanterman-Petris Short Act, protecting the rights of people with developmental disabilities.<sup>1</sup>

In 1972, California began to emerge as a national leader in privacy rights when it used the initiative process to explicitly add privacy to Article 1, section 1, of the California State Constitution. Privacy was added to the list of inalienable rights saying "...these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." 1972 also saw the Supreme Court privacy case *Eisenstadt v. Baird*, which affirmed the right to privacy under the US Constitution for all individuals, regardless of marital status. In 1974 the federal government passed the Privacy Act of 1974 and FERPA, protecting information collected by federal agencies and the privacy of student education records maintained by all schools receiving funds from the U.S. Department of Education. One year later the federal government promulgated 42 CFR Part 2, which added some of the strictest privacy protections privacy practitioners work with and provides critical protections for vulnerable groups who are receiving substance abuse treatment.<sup>2</sup>

In 1977, California enacted the Information Practices Act, which is analogous to the federal Privacy Act of 1974. This legislation establishes standards and requirements governing how the California government handles and utilizes the information of Californians. California then

---

<sup>1</sup> *History of Privacy Timeline* (2023) University of Michigan <<https://safecomputing.umich.edu/privacy/history-of-privacy-timeline>> (as of March 12, 2023).

<sup>2</sup> *Id.*

enacted the Confidentiality of Medical Information Act in 1981 which created a comprehensive state-level privacy protection for medical information. In 1986, the Telephone Consumer Protection act was passed along with the creation of the Do Not Call Registry, with both of these laws protecting against solicitation calls and allowing consumers to opt out of telemarketing calls. Privacy protections continued to grow globally in the 1990s with updates to the Human Subject Research requirements in 1991 to create the Common Rule which included research participant privacy standards. In 1995, The European Union Data Protection Directive was passed in the EU, and HIPAA was passed in 1996 to create somewhat comprehensive federal health information privacy and information security standards. In 1998, the Children’s Online Privacy Protection Act was enacted federally to provide protection to children when using the internet. The federal government then passed the Gramm Leach Bliley Act in 1999, requiring disclosure of how financial institutions share customer data, and gave customers the opportunity to opt out of having their information shared. The California Online Privacy Protection Act of 2003 was the first state law requiring websites to have privacy policies. The Red Flags Rule was passed in 2008 requiring financial institutions and creditors to develop written identity theft prevention programs. Then in 2018, the European Union’s General Data Protection Regulation was implemented to provide expanded privacy rights in the European Union,<sup>3</sup> and the California Consumer Privacy Act (CCPA) was passed to give consumers more control over personal information that businesses in California collect about them. The CCPA included rights to delete personal information collected from individuals, to know what personal information a business has collected and how it is used and shared, to opt-out of the sale and sharing of personal information, and to non-discrimination for exercising CCPA rights.<sup>4</sup>

Finally, since 2020, the Privacy Law landscape has witnessed an increasing pace of change and complexity. In August 2020, the California Department of Justice issued implementing regulations for the CCPA, and in November of the same year, the California Privacy Rights Act (CPRA), amending the CCPA, was enacted. The CPRA was passed by proposition and added rights to correct inaccurate personal information maintained by businesses in California, and rights to limit the use and disclosure of sensitive personal information. In March of 2021, the CCPA regulations were amended. In September of 2021, California passed the Genetic Information Privacy Act which covers direct-to-consumer genetic testing. In January of 2023, the CPRA went into effect in California, and the California Privacy Protection Agency (CPPA) – the newly established enforcement agency for the CCPA - promulgated implementing regulations.<sup>5</sup> The CPPA also requested comments on another rulemaking file addressing cybersecurity audits and risk assessments, and automated decision-making. Enforcement actions regarding the CPRA are currently scheduled to begin in March of 2024. At a national level, in only the first half of 2023, six more states have passed new comprehensive privacy laws.<sup>6</sup> At an international level, 71%, or 137 out of 194 countries have data protection and privacy legislation enacted, and 9% more have

---

<sup>3</sup> *Id.*

<sup>4</sup> *Frequently Asked Questions (FAQs)* (2023) California Privacy Protection Agency < <https://cppa.ca.gov/faq.html> > (as of March 12, 2023).

<sup>5</sup> *Id.*

<sup>6</sup> *Q2 Privacy Update: AI Takes Center Stage, plus Six New US State Laws* (Aug. 16, 2023) < <https://www.tripwire.com/state-of-security/q2-privacy-update-ai-takes-center-stage-plus-six-new-us-state-laws> >.

draft legislation under consideration.<sup>7</sup> The pace of change in the privacy law sector has never been greater and the landscape is only growing in complexity.

## NECESSITY OF A PRIVACY LAW SPECIALTY

The introduction of a specialty area in Privacy Law in California is essential for several reasons:

1. **Expertise in a Rapidly Evolving Field:** The dynamic nature of privacy law demands specialized practitioners who can stay abreast of the latest developments, ensuring clients receive accurate and up-to-date advice.
2. **Protection of Individual Rights:** Recognizing Privacy Law as a specialty area demonstrates a commitment to safeguarding individual rights and ensuring fair representation in matters concerning personal data protection.
3. **Legal Excellence and Ethical Standards:** By establishing rigorous criteria for specialization, the California legal profession will elevate its standard of excellence and ethical conduct in privacy-related matters.
4. **Business and Consumer Confidence:** Organizations will benefit from specialized legal counsel that can help them comply with privacy regulations, reduce legal risks, and build trust with their customers. Consumers will have increased confidence that attorneys who specialize in this area are best suited to handle these legal matters.
5. **Consistent and Preparatory Training:** Empower the development of an educational curriculum with the goal of ensuring that specialists are consistently trained and prepared to excel in this emerging field.
6. **California is a Technology Leader:** California's position as a technology leader and its early adoption of comprehensive privacy laws have solidified its status as a needed specialty area in privacy law, influencing not only other states, but also international discussions on data protection and privacy. This creates a need for consumer and vendor protection.

The proposed specialty area in Privacy Law will encompass a comprehensive curriculum covering key aspects, such as:

1. **Foundational Knowledge:** A solid understanding of privacy laws, regulations, and enforcement mechanisms at both state and federal levels.
2. **Data Protection Compliance:** Expertise in advising clients on developing and implementing

---

<sup>7</sup>*Data Protection and Privacy Legislation Worldwide* (Dec. 14, 2021) United Nations Conference on Trade and Development, <https://unctad.org/page/data-protection-and-privacy-legislationworldwide> (as of Feb. 13, 2023).

privacy policies, compliance programs, and risk management strategies.

3. Data Breach Incident Response: Specialized training in assisting clients in responding to data breaches, conducting investigations, and mitigating damages.

4. Privacy Litigation and Dispute Resolution: Proficiency in handling privacy-related litigation, including privacy class actions and disputes.

5. Emerging Technologies: An understanding of the impact of emerging technologies, such as artificial intelligence and the Internet of Things, on privacy and data protection.

The approval of a new specialty area in Privacy Law by the California Board of Legal Specialization is a forward-thinking step towards addressing the critical issues surrounding data privacy. By recognizing the significance of this field and fostering the development of specialized expertise, California will lead the way in protecting individual rights and ensuring legal excellence in privacy matters.

## AREAS/THEMES EXPLORED

Specializing in Privacy Law offers benefits such as a growing demand for experts in an increasingly digital world, the potential for high-impact work on important societal issues, and the chance to work with cutting-edge technologies. However, challenges might include navigating complex and evolving regulations, balancing conflicting interests, and addressing the international nature of data flow while dealing with varying legal frameworks across jurisdictions.

While researching the need for, and interest in, a California Privacy Law Specialist designation, the Privacy Law Group reviewed data pertaining to (1) other states with privacy law specializations, (2) bar associations and trade associations with privacy specialists, (3) California privacy cases, (4) enforcement actions with a privacy focus, and (5) public interest and advocacy groups with privacy focus. The group concluded there is significant interest and a compelling need for such the specialty area.

Information gathered from various jurisdictions reveals a spectrum of accreditation practices: some states recognize or mandate privacy law specialization accredited by the ABA<sup>8</sup>, some states maintain their own state-specific accreditations<sup>9</sup>, while two states prohibit specialization.

Some examples of specific programs include:

- Three states – Alabama, Minnesota, and Texas – have formally adopted a Privacy Law specialization accredited by the ABA via IAPP called PLS, which requires

---

<sup>8</sup> The American bar Association (ABA) has accredited the International Association of Privacy Professionals (IAPP) to certify lawyers in Privacy Law. <https://iapp.org/pls/>

<sup>9</sup> <https://www.americanbar.org/groups/specialization/state-sources-of-certification/certification-by-state/>

licensure, substantial involvement in privacy law, continuing education, peer references, the IAPP CIPP/US exam and a CIPM or CIPT designation from the IAPP, and an ethics exam.

- Six states/territories – Alaska, Arkansas, Delaware, the District of Columbia, South Dakota, and Tennessee list Privacy Law as a specialization that may be achieved via an ABA-accredited program like the IAPP’s PLS Program<sup>10</sup>.
- North Carolina has adopted their own requirements: North Carolina’s Privacy and Information Security Law specialization requires licensure, substantial involvement in privacy and information security law, continuing education, peer review, and both the IAPP CIPP US exam and a specific North Carolina exam<sup>11</sup>.

While the data is varied in specific applicable standards, it is clear that privacy law specialization is appreciated and supported by many jurisdictions across the United States.

In reviewing bar associations with privacy specialties, the Privacy Law Group identified no less than twenty active local and national privacy associations with dedicated sections and committees devoted specifically to privacy law.<sup>12</sup>

The Privacy Law Group also reviewed cases with a privacy focus to identify the ongoing legal need in California for privacy specialization, and in doing so focused on causes of action based on the CCPA, CMIA and Invasion of Privacy Act over the preceding three years. The PLG identified 34 CCPA cases with 13 filed in federal court and nine being class actions.<sup>13</sup> 49 cases, with 26 filed in federal court and 35 class actions were brought under the CMIA. Finally, 60 federal cases were filed under the CIPA, with 58 being putative class actions. As such, there is ongoing significant privacy-related litigation.

In reviewing enforcement actions with a privacy focus, another major driver for the need of legal expertise in privacy law, the Privacy Law Group identified significant and growing enforcement activity. In addition to the numerous and varying international authorities, the group identified seven major domestic enforcement entities and entity types: state attorneys general, state regulatory departments (e.g., CPPA, CDPHH, CPPA), the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Federal Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), and the Department of Health and Human Services (HHS). Each of the entities is responsible for specific enforcement actions based on industry-specific privacy statutes and regulations, but there is some significant overlap in jurisdiction, which can lead to complicated compliance requirements for the regulated public. A single privacy breach frequently requires reporting to multiple oversight entities at different levels of government with different reporting requirements and timelines.

<sup>10</sup> <https://www.americanbar.org/groups/specialization/state-sources-of-certification/certification-by-state/>

<sup>11</sup> <https://www.nclawspecialists.gov/for-lawyers/certification-standard-summaries/privacy-and-information-security-law>

<sup>12</sup> [See Review and Discussion of Member Research Regarding Bar Associations in California with Privacy Law Focus, Consulting Group on the Establishment of a Legal Specialization in Privacy Law \(Jun. 1, 2023\) <https://board.calbar.ca.gov/Agenda.aspx?id=16972&tid=0&show=100035609#10044181>.](#)

<sup>13</sup> The PLG notes that due to the relatively young CCPA and regulatory enforcement actions being delayed until 2024, the number of cases brought under CCPA or that are CCPA-related is likely to substantially increase over the next 3-5 years.



The Privacy Law Group's review of public interest and advocacy groups with a privacy focus also supported moving forward with the development of a privacy law specialization.<sup>14</sup> The group identified a number of interest groups at both the national and state levels. The International Association of Privacy Professionals, American Bar Association, Electronic Discovery Institute, Center for Democracy & Technology, Electronic Privacy Information Center, Data & Society Research Institute, Cyber Civil Rights Initiative, Access Now, Center for Digital Democracy, Center for Data Innovation, Privacy International, Global Network Initiative, Future of Privacy Forum, and Information Accountability Foundation all make significant contributions to privacy awareness and advocacy at a national and international level. California, as a privacy leader, is home to a variety of major privacy advocacy groups including the Electronic Frontier Foundation, Privacy Rights Clearinghouse, Californians for Consumer Privacy, and the World Privacy Forum.

In reviewing the value of a discrete privacy law specialty, the group also reviewed privacy as a defined area of the law to ensure that defined specific standards could be created and maintained, and the group found that privacy is defined as an area of the law. As outlined in the history of privacy law above, privacy has specific, defined, Constitutional, case-law based, and statutory and regulatory provisions. Additionally, the group found that at least seventeen major law schools and colleges teach privacy as a discrete topic with its own curriculum, including Stanford Law School, University of California, Berkeley, School of Law, University of California, Los Angeles, School of Law, University of Southern California Gould School of Law, Santa Clara University School of Law, and Golden Gate University School of Law. Federally, the United States House Committee on Energy and Commerce Subcommittee on Innovation, Data, and Commerce, the U.S. Senate Committee on Commerce, Science and Transportation Subcommittee on Consumer Protection, Product Safety, and Data Security, and the U.S. Senate Committee on the Judiciary Subcommittee on Privacy, Technology, & the Law are major contributors to federal privacy policy. At the state level California's State Assembly Committee on Privacy and Consumer Protection and Select Committee on Cybersecurity provide guidance on state privacy issues.

The Privacy Law Group concluded that there is a large and growing need for privacy law specialization and representation in California, a dedicated community of attorneys interested in and devoted to privacy law specialization, an area of law being refined by state and national communities and interest groups, and support for the growth of privacy law as a field for the long term within the legal community and education system.

## RECOMMENDATIONS

As technology continues to advance and data privacy becomes an increasingly critical concern, the recognition of Privacy Law as a specialized practice area is of utmost importance.

---

<sup>14</sup> While identifying a large number of public interest and advocacy groups focused on privacy law, the Group also noted a clear significant need for data privacy expertise among general legal aid groups and similar public interest and nonprofit organizations where data privacy questions are raised on a regular basis.

Privacy issues, both on a national and global scale, have become more complex in recent years. The evolving landscape of data protection laws, cybersecurity threats, and the widespread collection and usage of personal information by companies, governments, and individuals necessitate specialized expertise in handling privacy-related legal matters.

By approving Privacy Law as a specialty area, the California Board of Legal Specialization would pave the way for developing a cadre of legal professionals well-versed in privacy regulations, compliance requirements, and data breach incidents. This, in turn, would enhance the quality of legal representation for clients facing privacy-related concerns and promote a more robust protection of individual rights.

The benefits of recognizing Privacy law as a specialty area extend beyond the legal profession. Businesses operating in California would gain access to specialized legal expertise, enabling them to navigate the complexities of privacy regulations effectively. Additionally, consumers would benefit from heightened protection and confidence that their personal data is handled responsibly.

Privacy Law, as a distinct specialty, aligns with the principles of maintaining public trust, upholding privacy rights, and addressing emerging challenges in our digital age. It is a fundamental step towards ensuring a fair and just legal system that adequately addresses the intricacies of privacy matters.

The Consulting Group on the Establishment of a Legal Specialization in Privacy Law (PLG) strongly urges the California Board of Legal Specialization to approve the establishment of Privacy Law as a designated specialty area. Taking such action would demonstrate a forward-thinking dedication to protecting individual privacy, promoting legal excellence, and adjusting to the constantly evolving landscape of modern society.

The Privacy Law Group recommends proceeding to develop a California Privacy Law Specialist designation. There is a rising and substantial demand for certified privacy expertise within the legal field, offering significant value to California consumers through the development of this specialization. Furthermore, the realm of privacy law, although closely connected to various other legal domains, maintains its distinctive and well-defined character as a legal discipline. It boasts a substantial and expanding community of privacy law practitioners who would endorse and recognize the significance of a specialized focus in privacy law. The establishment and upkeep of standards and criteria for such specialization are both practical and highly sought-after, offering substantial benefits to Californians and legal professionals alike.

## MEMBERS

Member	Member Category/Type
<b>Jeewon Serrato, Chair</b>	Member Attorney
<b>Ryan Nathaniel Davis, Vice-Chair</b>	Member Attorney

<b>Soyeun D. Choi</b>	Member Attorney
<b>Robert Hershenson</b>	Public Member
<b>Michael Andrew Iseri</b>	Member Attorney
<b>Myriah Jaworski</b>	Member Attorney
<b>Hillary Noll Kalay</b>	Member Attorney
<b>Arsen Kourinian</b>	Member Attorney
<b>Linsey Krolik</b>	Member Attorney
<b>Paul Lanois</b>	Member Attorney
<b>Jesus E. Martinez</b>	Member Attorney
<b>Smita Rajmohan</b>	Member Attorney
<b>Oliver Unaka</b>	Public Member

## REQUIREMENTS FOR ESTABLISHING PRIVACY LAW SPECIALIZATION

To become proficient in Privacy Law, staff recommend developing several key requirements that need to be explored. Below is a list of sample requirements.

1. Curriculum: PLG should outline exam specifications needed for specialists to become certified in the area. PLG can explore topics from law school courses, sections' continuing education course offerings, and their like.
2. Exam Development: Developing an exam for privacy law involves careful consideration of the subject matter, the desired learning outcomes, and the level of expertise being assessed. A determination of what the minimum level of competence is required to demonstrate expertise in privacy law would need to be established. Here's an outline of the process:
  - A. Define Learning Objectives: Determine what the exam should to measure. Is PLG testing knowledge of specific laws, practical application, critical thinking, or a combination?
  - B. Select Topics: Identify key topics within privacy law that align with the learning objectives. These could include data protection regulations, compliance strategies, case law, ethical considerations, and more.
  - C. Create Questions: Develop a variety of question types to assess different skills. These might include multiple-choice, true/false, short answer, essay, case analysis, and scenario-based questions.
  - D. Design Questions: Craft clear, concise, and relevant questions. Ensure that each

question aligns with a specific learning objective. Avoid ambiguous language that might confuse test-takers.

E. Consider Difficulty Levels: Balance the difficulty of questions to reflect the level of expertise being assessed. Include easy, moderate, and challenging questions.

F. Include Real-World Scenarios: Use case studies or scenarios to assess how well candidates can apply their knowledge to practical situations.

G. Cover Diverse Content: Ensure a comprehensive coverage of the privacy law landscape, including different regulations, sectors, and emerging trends.

H. Avoid Bias: Craft questions that do not favor any specific perspective or point of view.

I. Create a Clear Structure: Organize questions logically and provide clear instructions for each question type.

J. Review and Edit: Review the exam for accuracy, clarity, and coherence. Ensure that questions are free from errors and that they accurately assess the intended skills and knowledge.

K. Pretesting: Administer the exam to a small group of test-takers to identify any issues or ambiguities. Use their feedback to make necessary adjustments.

L. Establish Grading Criteria: Define how each question will be graded, especially for open-ended or essay questions. Develop a rubric that outlines the criteria for awarding points.

M. Consider Time Constraints: Determine the appropriate time limit for the exam, ensuring it allows sufficient time for candidates to answer all questions.

N. Continuous Improvement: After the exam, review the results to identify areas where candidates performed well and areas where improvement is needed. Use this information to refine your exam for future iterations.

3. Minimum Trial or Practice Experience: The minimum trial or practice experience required for a privacy law specialist should be five years of legal work in the area and has devoted 25% of the time to practice in the specialty area. However, here's a general outline of the factors that might influence the trial experience needed to specialize in privacy law:

A. Foundational Legal Experience: Before specializing in privacy law, attorneys often gain foundational experience in general litigation, corporate law, or related areas. This

experience can provide a solid legal background and exposure to courtroom proceedings or transactional work.

B. Understanding of Privacy Law: Attorneys should have a strong understanding of the specific privacy laws and regulations that apply in their jurisdiction. This includes both domestic regulations (such as FTC Act federally or CCPA in California) and international data protection standards (such as GDPR in Europe).

C. Privacy-Related Litigation or Transactional Experience: To be a privacy law specialist, having experience in litigation or transactional experience is valuable. Litigation experience might involve representing clients in court, handling discovery, drafting pleadings, and participating in trials or hearings. Transactional experience might involve drafting and negotiating contractual agreements, reviewing, and advising clients on new product development, and advising clients on developing and implementing compliance programs and risk management strategies.

E. Case or Project Complexity: The complexity of cases or projects handled can influence the level of experience required. In certain privacy law cases or projects, attorneys may encounter considerable complexity, necessitating the navigation of technical details and nuanced legal arguments or approaches.

F. Level of Responsibility: Attorneys may start with supporting roles in privacy-related litigation or transactions, gaining experience by assisting senior lawyers. As they gain more experience and demonstrate their skills, they might take on greater responsibilities. This could involve briefing executives or board of directors.

G. Negotiation and Settlement: In some instances, privacy-related cases might not go to trial but are settled through negotiation or alternative dispute resolution methods. Experience in negotiation, mediation, and settlement processes is also valuable for privacy law specialists.

H. Industry Expertise: Depending on the industry or sector, privacy law cases can vary significantly. Having experience in specific industries (e.g., healthcare, finance, specific technology) can enhance an attorney's specialization.

4. Peer References or Review: Some number of peers who are familiar with the competence and qualification of the attorney in privacy law could be required. Certain requirements could be developed for who qualifies as a peer for this purpose could be developed, such as being licensed and in good standing to practice law, having significant legal experience in privacy law, and not related by blood or marriage to the applicant or not being a current

colleague at the attorney's place of employment.

The future state of privacy law may face challenges such as keeping up with rapidly evolving technology, balancing individual privacy with societal interests, and harmonizing regulations across different jurisdictions. Additionally, addressing issues related to data breaches, surveillance, and the ethical use of emerging technologies like AI could pose significant hurdles for privacy legislation.

## CONCLUSION

As this report states and the presentations provided at the scheduled meeting, PLG has established that there is a need to move forward with a recommendation to adopt this as a new specialization to the CBLs. Several other factors contribute to the recommendation of Privacy Law, including the California Lawyers Association (CLA), other national programs that can serve as models, such as the North Carolina State Bar Legal Specialization, and the interest from the public, as well as from attorneys.

State Bar Rule 3.116(C) dictates that with the establishment of a new specialization area, the State Bar may approve for a period of no more than two years satisfactory completion of one or more alternative tasks in lieu of a written examination. Should the CBLs approve the recommendation to add Privacy Law as a specialty area, the PLG will need to recommend the certification specifications, experience requirements, continuing legal education subfields, and the alternative requirements.

In summary, choosing to specialize in privacy law presents a rewarding path replete with compelling advantages. In our increasingly interconnected and data-driven world, the demand for privacy experts continues to soar. This specialization offers a chance to play a pivotal role in protecting individual rights and influencing the responsible utilization of technology. Nonetheless, it's imperative to recognize the accompanying challenges, including navigating a dynamic regulatory landscape and devising strategies to tackle the global dimensions of data privacy concerns. With the potential to wield a substantial influence and contribute to a more ethical and secure digital future, the field of privacy law specialization emerges as an enticing and indispensable avenue for legal professionals to explore.