IAPP Privacy Law Specialist Designation

Prepared for Delegates to the American Bar Association House of Delegates
May 2017

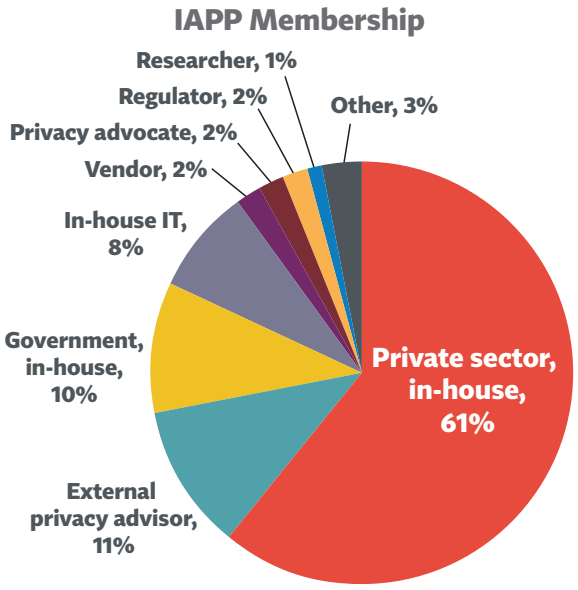
iapp

The International Association of Privacy Professionals (IAPP) is respectfully applying for the ABA's approval of its new Privacy Law Specialist designation, which is based on individual attorneys passing certification exams, demonstrating multiple years of law practice experience, and submitting professional references, as explained below. The approval is intended to authorize lawyers to list the designation alongside their name on their business cards, online profiles, professional websites, or email signature lines, while complying with the Model Rules of Professional Conduct provisions on Communication of Fields of Practice and Specialization. The IAPP's Privacy Law Specialist designation has met the ABA's Standards for Specialty Certifications for Lawyers, according to the Standing Committee on Specialization, and the Committee's resolution in favor of the IAPP's application awaits approval of the ABA House of Delegates.

What is the IAPP?

The IAPP is a not-for-profit professional membership association headquartered in Portsmouth, New Hampshire. With more than 29,000 members worldwide and 100 full time employees, the IAPP also has offices in Ottawa, Brussels, Mexico City and Singapore. The IAPP's mission is to define, promote and improve the privacy profession globally. It is a policy neutral, non-advocacy organization with members from government and the private sector, ranging across numerous industries, and including practitioners, academics, regulators, and civil society representatives. The IAPP offers its members privacy training and certification; content resources ranging from daily newsletters to original in-depth research, practice guides and professional tools; five annual conferences globally in the U.S., EU and Asia; networking opportunities across more than a hundred local chapters around the world; and more.

According to its 2016 annual privacy governance report, more than 60 percent of the IAPP's members work in-house for the private sector. Outside counsel and consultants represent approximately 11 percent of the IAPP membership, with in-house government sector employees comprising another 10 percent.



What IAPP certifications are required for the Privacy Law Specialist designation?

The IAPP has offered certifications in information privacy for more than a decade, and many lawyers already hold these certifications. The principal certification is the Certified Information Privacy Professional (CIPP), of which there are now multiple designations to accommodate the global nature of privacy and data protection law. The IAPP offers CIPP United States/private sector (CIPP/US), as well as CIPP/US Government (CIPP/G), Canada (CIPP/C), Europe (CIPP/E), and Asia (CIPP/A).

Because privacy is a multi-disciplinary profession, the IAPP also offers training and certification in information privacy program management (the CIPM). With the CIPP covering the "what" of privacy, the CIPM covers the "how." It addresses the implementation of establishing a reliable and measurable privacy program on behalf of an organization. Attorneys use these skills routinely.

The Certified Information Privacy Technologist (CIPT) exam is designed to address the technical side of privacy, another core component of privacy literacy for privacy lawyers.

The CIPP/US, CIPM and CIPT exams are accredited by the American National Standards Institute (ANSI). This accreditation involves an in-depth evaluation of the IAPP's certification exams, testing policies, procedures, and staff, and ongoing reviews to ensure compliance. ANSI accreditation indicates that the IAPP's certification examinations meet the stringent ISO/IEC 17024:2012 standards. The ANSI accreditation letter is attached as Appendix 1.

In order to meet the minimum requirements of the Privacy Law Specialist designation, an attorney must pass the CIPP/US exam and either the CIPM or the CIPT exam.

In addition to passing two IAPP exams, what else is required of attorneys seeking Privacy Law Specialist designation?

An attorney cannot earn the Privacy Law Specialist designation simply by passing the IAPP's ANSI accredited certification exams. The IAPP readily acknowledges that lawyers—and non-lawyers—could pass the exams with sufficient preparation time, even if they have not developed professional expertise in the field. For example, in the past few years, law students have increasingly taken and passed the exams in order to improve their career opportunities in privacy. Passage of the CIPP/US and either the CIPM or CIPT, then, is necessary but not sufficient to meet the Privacy Law Specialist requirements.

In order to earn the Privacy Law Specialist designation, U.S. attorneys in good standing who hold two qualified IAPP certifications must also:

- **Pass an IAPP exam covering aspects of the Rules of Professional Conduct.** The exam is designed to reflect common ethical issues in-house and outside counsel face in practicing Privacy Law. This requirement may instead be met by proof of a score of 80 or higher, within the past five years, on the Multistate Professional Responsibility Exam (MPRE). The IAPP's Privacy Ethics exam was created in collaboration with a volunteer group of experienced

privacy attorneys representing in-house and outside counsel practices, and was vetted with law students who had recently studied for or taken the MPRE and/or had completed a Professional Responsibility course.

- **Submit in writing a demonstration that the attorney has been "substantially involved" in the practice of Privacy Law.** The practice must be a significant component of the applicant's full-time law practice for at least the prior three years. The "substantial involvement" requirement was defined by a panel of volunteer attorneys – again, both in-house and outside counsel – from the IAPP's Privacy Bar Section. It went through several iterations with the ABA Standing Committee on Specialization before it met the committee's standards. The current definition reflects the activities most commonly fulfilled by attorneys practicing Privacy Law. Of course privacy laws differ depending on the statutes and regulations involved, but there is a common core of activities in which all privacy lawyers engage. A detailed definition of "substantial involvement in the practice of privacy law" is attached as Appendix 2.

- **Submit evidence of at least 36 hours of participation in qualified continuing legal education in the field of Privacy Law in the three-year period preceding the application date.** Qualified courses include: (a) sessions on privacy law and privacy law practice offered at IAPP conferences; (b) a meeting or conference hosted or recommended by one of the ABA subcommittees of the Science and Technology

The IAPP developed the Privacy Law Specialist program in response to requests by several attorney members who wanted to verify that use of the CIPP/US designation on business cards, online profiles, professional websites or email signature lines complies with Section 7.4 of the Model Rules of Professional Conduct. To assure lawyer members that they could publicly communicate their IAPP credentialing, the IAPP sought ABA accreditation.

For this, the IAPP developed a program to meet the ABA's Standards on Attorney Specialization and applied to the ABA Standing Committee on Specialization for review and ultimate approval. This program, which is now ready to be deployed, is designed to apply uniquely to U.S. lawyers who have been practicing Privacy Law consistently for several years and can demonstrate their competence and experience in the field.

Attorneys who have passed the CIPP/US exam and one of the other required exams will not automatically qualify for the new credential, as candidates may not have the requisite years of qualified privacy practice. Moreover, many seasoned privacy attorneys may not seek the credential, because IAPP certifications are more common among in-house counsel.

What is at issue is whether the components of the IAPP's Privacy Law Specialist designation meet the ABA's specialization criteria. If they do, then a lawyer who wishes to obtain the specialization designation will be permitted under many states' rules of professional conduct to post the designation in their public communications.

Section that focuses on information technology, privacy or security; (c) a law school course taught or attended by the applicant at an ABA accredited law school; (d) a seminar, workshop, panel or other CLE attended by or taught by the applicant to an audience primarily consisting of attorneys; or (e) published books or scholarly articles in the field of privacy (blog posts and related short-form, news-like publications are excluded).

- **Provide at least five but no more than eight peer references.** The references must attest to the applicant's qualifications and "substantial involvement" in the practice of Privacy Law. "Peers" include other attorneys, regulators, clients, or judges who can personally attest to applicant's qualifications.

Why did the IAPP pursue a Privacy Law Specialty?

The IAPP created the "Privacy Law Specialist" program to accommodate the requests of lawyer members who hold IAPP certifications and would like to list the designation alongside their name on their business cards, online profiles, professional websites or email signature lines, while complying with the Model Rules of Professional Conduct provisions on Communication of Fields of Practice and Specialization. The IAPP estimates that approximately 40 percent of its members are attorneys.

Over the past two decades, information privacy has grown as a professional field in the U.S., based on a series of federal and state laws and regulations covering how organizations collect, use, share, transfer internationally, and store personal information. These laws and regulations respond to the challenges wrought by the Information Age, including the exchange of personal information for goods and services, the growth of Big Data analytics in target marketing, security vulnerabilities associated with data stored on internet-connected servers, and the ubiquity of cross-border data transfers in a global economy.

Several ABA accredited law schools now offer courses and programs in Privacy Law, including but not limited to: Santa Clara School of Law; the University of Minnesota School of Law; Georgetown School of Law; and the University of Maine School of Law. Santa Clara and Maine Law each offer a Certificate in Privacy Law. The John Marshall School of Law offers an LLM in Information Technology and Privacy Law. Two years ago, the IAPP launched its Privacy Bar Section to serve the specific needs of attorneys practicing in the field. In addition, it hosts the Privacy Pathways program with several law schools that provide support for their students seeking careers in privacy law.

The IAPP's Privacy Law Specialist designation program has undergone review by the ABA Standing Committee on Specialization. Its exams have been reviewed by Ohio State University law professor Dennis Hirsch, who is one of the leading scholars in the privacy legal academy. The Standing Committee has unanimously recommended approval by the ABA House of Delegates of the IAPP's designation, as meeting the ABA's Standards for Specialization accreditation.

How does the IAPP describe the designation?

The IAPP will provide the following information to attorneys seeking the Privacy Law Specialist designation:

> The Privacy Law Specialist designation signifies substantial time practicing U.S. state and federal law relating to safeguarding personal information; knowledge of relevant privacy laws, regulations, and technology; and a commitment to staying abreast of new developments.

Accreditation by the ABA indicates solely that the IAPP's Privacy Law Specialist designation has met ABA standards.

Not all states allow attorneys to claim specialization even if certified by an ABA accredited body like the IAPP. Lawyers should check the Rules of Professional Conduct of their state (typically covered in Rule 7) to see what their state's requirements are with respect to communicating fields of practice and specialization.

How will an attorney advertise the Privacy Law Specialist designation?

Model Rule 7.4 provides: "(d) A lawyer shall not state or imply that a lawyer is certified as a specialist in a particular field of law, unless: (1) the lawyer has been certified as a specialist by an organization that has been approved by an appropriate state authority or that has been accredited by the American Bar Association; and (2) the name of the certifying organization is clearly identified in the communication."

Attorneys who are certified by the IAPP as a specialist will therefore have to identify the IAPP as conferring the "Privacy Law Specialist" designation.

Appendix 1

August 05, 2015

Ms. Marla Berry
International Association of Privacy Professionals, Inc.
75 Rochester Ave., Suite 4,
Portsmouth, NH 03801, USA, USA

Dear Ms. Berry:

The ANSI Personnel Certification Accreditation Committee (PCAC) reviewed the assessors' report for the International Association of Privacy Professionals, Inc.'s (IAPP) 2014 surveillance for initial accreditation. PCAC held an online ballot and voted to accept the assessors' recommendation to close all nonconformities and grant IAPP accreditation under the ISO/IEC 17024:2012 standard.

On behalf of ANSI, I would like to extend our congratulations on this achievement. We look forward to a continued partnership with the International Association of Privacy Professionals, Inc.

If you have any questions about IAPP's accreditation, please do not hesitate to contact me.

Sincerely,

D. Hardmon-Fort

DeMario Hardmon-Fort
Program Coordinator, Personnel Certification Accreditation Programs

CC: Steven Peluso, PCAC Chair
Lynn Webb, Ed.D, Lead Assessor
Michael Boggs, Assessor
Thomas Adams, Lead Reviewer
Linda Nober, Ph.D., Reviewer

Appendix 2

Definition of "substantial involvement in the practice of Privacy Law," as approved by the ABA Standing Committee on Specialization:

Applicant must demonstrate (in a manner that does not reveal confidential and privileged information) that Applicant has been actively engaged in the practice of privacy law either as a transactional lawyer, in privacy program management, privacy litigation or regulatory practice, or a combination of these. Active engagement in information security law will also be considered provided Applicant demonstrates its connection to and role in the privacy specialization.

Applicant must demonstrate that Applicant has both quantitative and qualitative substantial involvement in the field. In particular, Applicant must declare and demonstrate through narrative description and through support letters that at least one-quarter (25%) of Applicant's full-time practice in each of the prior three years has been devoted to the practice of privacy law. In the narrative description, Applicant must provide specific examples of his or her engagement with the following types of privacy law practice activities:

For outside counsel and in-house lawyers with principally a transactional practice, at least 15% of Applicant's full time practice must include:

- *Preparation and review of privacy notices compliant with state, federal and/or international laws and regulations, and reflective of an organization's privacy practices, and privacy and security policy development, including development of information handling, sharing, storage, training, and security policies and programs (at least 5% of a full-time law practice);*
- *Contract development, negotiation, and compliance, which may include review of vendor, purchase, procurement, or acquisition contracts as well as drafting and negotiation of contracts for inclusion of privacy and security provisions (at least 5% of full time law practice); and*
- *Privacy advice in compliance with state and federal laws, including legal advice on privacy by design in product design or services (at least 5% of full-time law practice).*

Some elements of the 25% minimum may also include:

- *Conducting Privacy Impact Assessments and providing advice in connection with them;*
- *Risk assessment with regard to use and potential misuse of personally identifiable information, and corresponding legal advice to clients and organizational leadership;*

- *Counseling on cross-border data transfers, and other compliance with international privacy laws pertaining to data transfer (such as drafting Binding Corporate Rules, standard contractual contacts, certifying to US-EU Safe Harbor/Privacy Shield, and the like);*
- *Counseling on cybersecurity issues, breach preparedness, and breach remediation;*
- *Legislative or regulatory public policy engagement, which may include drafting of position papers or opinions, and interaction with legislative or regulatory bodies, which develop laws or regulate privacy practices;*
- *Advice about cyber insurance and negotiating cyber insurance policies.*

For attorneys primarily engaged in data breach response, adversarial proceedings and/or litigation, at least 20% of Applicant's full time practice must include:

- *Internal breach investigation and evaluation, involving managing internal investigations of data breaches and evaluating risks for mitigation and policy development, as well as engaging and overseeing the work of forensic teams, preparing breach notification letters, and working with regulators (at least 10% of full time law practice);*
- *Litigation of data protection and data breach matters in state, federal, international, and administrative tribunals (at least 5% of full time law practice); and*
- *Regulatory investigations and defense, including federal, state, or international filings of regulatory inquiries or responses to regulatory inquiries of privacy and data protection practices (at least 5% of full time law practice).*

Some elements of the 25% minimum may also include:

- *Privacy tort litigation such as litigation of consumer protection / privacy statutes that provide a private right of action (federal and state), including without limitation rights of publicity, rights against publication of false information, intrusion on seclusion, or public disclosure of private facts; and*
- *Advice about cyber insurance and negotiating cyber insurance policies.*