LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

August 2019

The State of the U.S. Privacy Job Market, 2019

A Reflection on the Year Behind, the Years Ahead and Why Privacy Means So Much to Us

By LJN STAFF

If orange is indeed the new black, then privacy might be the new cybersecurity. In just over a year since GDPR Day (May 25, 2018), privacy by design has made privacy as a profession one of the fastest growing and hottest verticals in and outside of the legal job market. Just as cybersecurity jobs are touted as having the highest demand yet lowest supply of talent in the American ecosystem, privacy is quickly becoming a field of increasing potential for talent in tertiary disciplines such as security, e-discovery, information governance, legal or compliance to find reinvention as well as greater vertical and financial mobility.

Few global legal phenomena in recent decades can compare to the sweeping impact the European Union's General Data Protection Regulation has had on big and small businesses alike, both domestic and abroad. GDPR has simultaneously been a job stimulus and an inflection point in how seriously society intends to govern our cultural, geopolitical and social identities as consumers. While U.S. law on data privacy is notably different and currently lacks federal regulation, a company's posture on data privacy has become vital to corporate brand identity — and arguably survival — in a changing global economy. Growth and maintenance of GDPR programs, fragmented updates in domestic privacy regulations, the increasing standardization and acceptance of training and education and an evolving American corporate commitment to consumer transparency around data collection will all alter the landscape of the privacy job market in the coming years. What we call and consider privacy today will enlarge and expand from this early origin, but for the near future, the impact will unquestionably mean more jobs.

What do those jobs entail? Who competes for those jobs? What is the mindset of the hiring managers when evaluating talent? How can someone transition into the space? Over the last half decade, TRU Staffing Partners has represented and continues to represent thousands of professionals and hundreds of opportunities in privacy. The following findings are from day-to-day talent assessment, staffing fulfillment, executive-level interviewing, collaborative job requisition creation and market intelligence and aim to capture the current state and predict the future of the privacy job market in the United States.

Current State

There are more people who self-identify as privacy professionals than one might think. The 2019 Global Privacy Summit hosted by the International Association of Privacy Professionals (IAPP) this April had well over 4,000 attendees, and IAPP membership has soared from roughly 36,000 members to an astounding 50,000+ since GDPR Day 2018. The IAPP plays a key role in the maintenance and professionalization of the privacy field. IAPP certifications are the gold standard for training and certification in privacy (CIPP, CIPM, CIPT, FIP, PLS). The IAPP also releases a compelling salary survey every two years. Here are some quick key takeaways from the 2019 report regarding compensation and education that resonate as real and true:

- Median salaries have risen by more than $8,000 since 2017 to $123,050, and additional compensation in the form of bonuses and raises has also increased — the median value of additional

Jared Coseglia is the founder and CEO of TRU Staffing Partners, an Inc 5000 Fastest Growing American Company 2016 & 2017 and National Law Journal's #1 Legal Staffing Agency. A member of our Board of Editors, he has over 15 years of experience representing thousands of professionals in e-discovery and cybersecurity throughout the world. Contact him at jared@trustaffingpartners.com.

compensation in 2018 was $20,000.
- Salaries are still highest in the U.S.: the median salary of a privacy pro is $150,000, up from $130,000 in 2017.
- U.S. chief privacy officers take in a median salary of $212,000.
- There is approximately an $80,000 difference between the median salary of CPOs and the median salary of non-CPOs.
- 42% of respondents hold a professional degree, such as an MBA, LL.M. or J.D.

Salaries over the last few years have certainly gone up for midlevel hires in privacy roles, and that is where most of the hiring occurs right now. Rewind to 2014 through 2017 and the volume of CPO or partner-level opportunities was quadruple what is available in 2019. Over the last several years, companies have hired or elevated individuals into executive-level leadership roles, and now those professionals are building teams. That does not mean the window of opportunity for a CPO-type role has evaporated, but it does mean the volume of those jobs has and will continue to diminish. This shift in hiring toward midlevel talent — often thought of as a senior associate within law firms or the manager/director level within corporations and consulting firms — will ultimately mean more jobs, but with significantly lower pay than CPOs. For the duration of 2019, the demand will remain high in these areas on the org chart.

To be in legal or not to be in legal? That is the question. Should the privacy function be within the legal department and should people handling all elements of privacy be lawyers? The former is a constant point of debate in the community (read some of that debate from Ruby Zefo, CPO of Uber, here), while the latter point is generally quickly dismissed. While lawyers do compete for jobs in privacy against nonlawyers, the current state of the privacy job market is largely operationalizing privacy by design throughout all segments of a business, which will continue to allow for many people not serving a legal counsel function to participate and lead. There is no question, however, that there are a lot of lawyers in the privacy space, both doing the hiring and being hired. The types of roles lawyers play, however, differ greatly between employer verticals.

There are four core employer verticals in the United States: corporations, law firms, service providers and government agencies. Different job trends occur in different sectors of the market, and the trends are best explored by separating and analyzing hiring behaviors in these four core silos. Opportunities are evenly found within all four segments, but the hiring profiles, desired skill sets, compensation ranges and timeline to hire differ vastly between each. For example, on the topic of geography, corporations generally want employees on-site, usually at the headquarters, while consulting firms and vendors are much more open to partial or complete remote work-from-home lifestyles. Across all four segments one thing remains consistent: Full-time direct-hire opportunities are being equally leveraged as contract staffing and part-time privacy talent augmentation.

What Is Happening In-House

Most major Fortune 1000 companies have a CPO or someone sitting in a role with the responsibilities of a CPO. The same holds true for a DPO. These two roles are rarely, if ever, filled by the same person. The IAPP eloquently describes the difference between the two by saying "the DPO role is shaping up to be a relatively low- or, at best, mid-level compliance position rather than a leadership or executive role, like the CPO or lead privacy counsel." Most corporations have these two positions filled. Sometimes the responsibilities of a CPO fall under the CISO (chief information security officer), the CCO (chief compliance officer) or often privacy counsel. (In this last role take Groupon's Brock Wanless, for example, and read "No CPO? No Problem!" here.)

Many of America's largest corporations have begun the operationalization of privacy beyond just leadership roles. This can include headcount directly attributed to a privacy program, but also, and often, "dotted-line" reports coming from various areas within the organization (HR, IT, marketing, security, compliance). Human capital within many companies may not be fully dedicated to privacy functions but may commit significant amounts of their time to privacy-related responsibilities, typically anywhere from 10% to 50% when partially leveraged. The story many companies tell is one of privacy leaders getting through GDPR by pulling resources from other departments. In a post GDPR-world, privacy leaders are fighting for buy-in and budget to make more meaningful hires. According to CPO Magazine's Data Protection and Privacy Officer Priorities Report 2019, 23% of respondents "have only one employee working in the data protection and privacy function." See more results from this survey in the sidebar, below.

Since approval for full-time headcount can be challenging, corporations are using contractors for privacy in a variety of different ways. Contract attorneys are being engaged for legal work specifically related to contract review and creation, policy writing and oversight of external

vendor contracts. Additionally, contract privacy pros who have built or participated in program design and operation often find themselves assisting corporations repair or uplevel their programs before exiting said temporary employment. The ecosystem for available contract privacy talent, both legal and nonlegal, is surprisingly vast as many seasoned privacy professionals are choosing consulting as their primary employment operandi, mirroring their entry-level counterparts who are more than willing to take part-time and contract opportunities to break into the space.

When direct headcount is granted, the responsibilities of a midlevel privacy professional at most corporations include ensuring regulatory privacy compliance, making the company accountable to industry best practices, the maturing of policies and standards, a heavy focus on internal training and awareness, consultative services like privacy impact assessments or governance risk compliance engagements and ongoing monitoring — specifically running and owning the GDPR program. CPOs are also evolving (a topic discussed in Future State) and need talent to step in and run the programs they have built.

In general, corporations want professionals with experience managing large, complex data governance projects, ideally with privacy experience or simply just privacy training. Hiring managers almost always ask for CIPP certification holders, and having a CIPP/US or E coupled with a CIPM almost guarantees a candidate's resume will get greater consideration than a candidate who does not have these certifications. The titles of director or program manager are often used, but there is not enough of a standard industry-wide to judge any job by its title. Job seekers are encouraged to understand the details of a job requisition — many of which are being handcrafted for the first time — before assuming the title makes them over- or underqualified.

What Is Happening in the Am Law 100

Most of the Am Law 100 law firms now have a privacy practice group. The practice may be inclusive or co-branded with security, risk or governance, but the efforts to provide niche legal counsel on privacy exist with partners in place at various levels of practice development and maturation. There are still opportunities to enter large and boutique law firms at a partner level if you have a book of business and clients who will follow. To break into larger Am Law firms, being able to bring talent with you on joining the firm as well as clients will undoubtedly make you more marketable.

The sweet spot for partner-tracked hiring at major U.S. law firms is around the three- to seven-year associate level. The average timeline to fill an Am Law privacy associate or senior associate hire is five to eight months, and for partners the process could take over a year of courtship and calculation. Am Law's top privacy practices generally want to poach talent and business from peer practice groups in other top firms. It is challenging for solo practitioners and aspiring privacy lawyers with no real experience to win these jobs. The privacy senior associate job market is one of musical chairs, and firms are mostly investing in proven talent.

This is not to say that law firms are not hiring staff attorneys and contract attorneys for privacy-related tasks — they are! Over the last year there was a spike in demand for contract talent with CCPA knowledge coupled with previous GDPR experience. Wise privacy lawyers looking for contract work are now getting savvy to the needs of the marketplace and proactively following the laws of each and every state, making them able to advise clients and contract to the highest-bidding law firm outsourcing this part of its legal practice. These same contractors, as mentioned above, are winning business directly from corporations doing the same or similar work. Another robust area of contract hiring for law firms is around contract review. This is not to be confused with contract attorney review in discovery. These privacy contract professionals are reviewing and editing contracts for law firms themselves and for their clients. Often these contractors manage security and privacy-related issues with the law firm's third-party vendors.

Part two of The State of the U.S. Privacy Job Market, 2019, next month, will outline what is happening in the privacy job market within service providers and government agencies as well as predict how a lack of federal regulations, training and education and evolving data governance demands will impact the future state of the U.S. privacy job market.

—❖—

Rachael Haher
Business Development Manager
TRU Staffing Partners
P: 718-541-3630
E: rachael@trustaffingpartners.com