

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

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

Part Two of a Two-Part Article

Part One of *The State of the U.S. Privacy Job Market, 2019* exposed the current state of the market, highlighting the expansive mid-market job growth and extensive use of contract talent resources, then drilled down into the nuances of staffing habits within U.S. corporations and major law firms. Part two of *The State of the U.S. Privacy Job Market, 2019* will outline what is happening within service providers, consultancies, and vendors will touch briefly on government agencies and will predict the near-future state of the U.S. privacy job market.

What Is Happening In Vendors/ Consulting Firms

The largest consulting firms in the world have been building privacy-focused consulting practices for over half a decade. These practices are often hatched from leaders in

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.

security, risk advisory, and e-discovery consulting — sometimes from outside/inside counsel — and now have dozens if not hundreds of disparately skilled privacy consultants ranking from entry level to seasoned partner. The war for privacy talent among these firms has begun and will continue in perpetuity. Consulting firms generally want to hire consultants from other consulting firms; that is traditionally first preference. There are opportunities for in-house corporate-tracked privacy professionals to transition into a major label in the global consulting firm ecosystem, but those without existing relationships and possible streams of revenue (and especially those without the desire or aptitude to *eventually* drive revenue) will struggle to transition at their desired compensation.

The market for privacy consulting is incredibly polarized. There are generally large consulting firms that do this work, from quasi-legal advisement to fully operationalizing and running privacy by design programs, and there are also a lot of boutiques. The large players in the space are certainly the “Big Four” but also all of their competitors such as BDO Global, FTI

Consulting, Booz Allen Hamilton, Aon, Accenture, BRG, Ankura, and many more. The maturity model of each consulting firm varies drastically from brand to brand, which has created opportunities for strong players at established practices to bring their expertise and clientele to midsized logos looking to invest in talent to grow faster. This has also allowed larger companies to begin investing in less experienced talent, grooming from within, and create newer, less expensive consultants to deploy to clients who are also in a heightened state of privacy maturity and now need lower rates for maintenance/impact assessment consulting work.

The cost and utilization necessary for more maintenance-oriented privacy consulting engagements become a key consideration for consulting firms' business models moving beyond GDPR day. What may have felt like corporate panic between mid-2017 to late 2018 appears to have ushered in a corporate acknowledgment and awareness of privacy as a necessary function and brand consideration, both operationally and strategically. Some corporations hire consultants from their consulting firms, bringing

the functions in house; this is an age-old practice. Others simply diminish the billable hours needed from their trusted consulting firm partners.

The nature of the work needed is also changing and often no longer requires the most senior of partners to be available to maintain the day-to-day privacy needs of the client. This is where contractors are playing a key role. Managing directors are bringing in temporary, often part-time resources to handle maintenance while they shift efforts to driving more revenue and personally billable consulting hours. The high-performing privacy contractor that can get patched into a consulting firm with multiple part-time accounts can quickly find more than enough hours to compensate for the concern of an inconsistent and unpredictable amount of billable hours.

Many established privacy pros, a vast majority of whom are lawyers or former CPOs/GCs at corporations, have decided to “hang out their shingle” and try their luck at building startup privacy practices all over the world. Many are sole owner/practitioners, some have grown to double-digit headcount, but almost all in this category are exploring the use of contract privacy augmentation for two reasons: One, they themselves become the contractor and lend their talents to a larger consulting firm, corporation, or law firm through a staffing agency; and/or two, they need to scale quickly when bidding on and winning business that changes the entire scope of necessary human capital needed to execute on new engagements.

Smaller companies often win government bids for contracts related to building privacy programs within

alphabet agencies. The privacy team is usually led by a tenured leader at the boutique firm, and the rest of the talent is often contractors. Winning federal bids usually means contracts have finite timelines, tough and potentially lengthy ones (one to three years). Offering a long-term contract is a comfortable modality for privacy pros accustomed to federal employment and, perhaps surprisingly, is something most actively job-seeking privacy professionals subscribe to comfortably. “Years” is a long time to someone who has chosen the contract lifestyle, and the privacy vertical is full of professionals who crave that lifestyle and occasionally, the stability of something as long-term as “years.”

Mid-level privacy professionals coming out of boutique consulting firms have tremendous opportunity to make a career move into a much larger consulting firm after getting even just a little experience. Lifestyle and job demand expectations can differ dramatically from small to giant employers, and privacy pros are well-advised to consider culture as much as cash when considering a next step. Privacy consultants coming from well-known logos are well-positioned to move in-house to corporations. The culture change between consulting firm and corporate client can also be notably jarring. The assumption that quality of life improves as you move from consultancy to corporation is often a false one. Every company, regardless of size, holds a different standard and expectation related to quality of life. Lawyers working at law firms who are beholden to the billable hour model likely maintain the lowest work/life balance, but some vendors have better balance than some

corporations and vice versa, regardless of industry vertical.

Future State

Several possible events can — or will — have a dramatic effect on the privacy job market in the next few years.

The most important variable in predicting the outlook of the U.S. privacy job market is the rapidly evolving state-by-state legislation sprouting across the country, standing in stark contrast to the lack of clearly impending federal regulation that can serve as one law to rule them all. Keeping up with all fifty individual state laws, plus international regulations can be taxing on companies, particularly smaller ones. (The International Association of Privacy Professionals [IAPP] has a great resource available to keep everyone updated on **state legislation status**.) Most privacy leaders want to see a federal U.S. privacy law for this very reason, but also because the disparity of state-mandated regulations contradicts one of the cornerstones of many Fortune 1000 privacy policy stances, which is: “Keep privacy simple.” For better or worse, this disparity is creating jobs, namely for the contract augmentation privacy lawyers within law firms and corporate legal departments (see **Part One**). With a presidential election looming and uncertainty around who will be in the White House in 2021, it may be years before meaningful federal legislation is passed to supersede the currently fragmented state data privacy laws. As a result, expect plenty of work for privacy lawyers in the future—direct-hire, contract-to-hire, and contract only.

Another event that will impact the privacy job market is the imminent

evolution of privacy leaders. The primary agenda for most newly minted CPOs in the last three years has been to build a privacy program, driven largely by the requirements of GDPR. Many organizations that did not have a privacy program prior to GDPR have one now, but many of the CPOs who built those programs have more to offer than the maintenance and gradual enhancement of the in-house privacy program and policies. Some CPOs are shifting upstream and becoming CDOs (Chief Data Officers) due to the success of the GDPR program development and the insight into corporation data-leveraging opportunities that the GDPR build exposed.

The focus of many privacy professionals is going to shift away from pure compliance and regulatory work and move to the monetization and strategic use of data to benefit the business. Leveraging data to benefit brand success sounds more like an information governance agenda than a privacy program responsibility, which points to the shifting leadership role in the dance between corporate privacy and information governance professionals, and privacy pros may now be taking the lead. The regulatory pressures and requirements of GDPR compliance forced a maturing of broader information governance policies and procedures, centered specifically on privacy. These corporate operations are now evolving to serve the organization in ways beyond GDPR compliance. Many companies lacked commitment and investment in operationalizing broad information governance initiatives because these programs were opportunistic, not mandated. That changed with GDPR, and privacy

professionals are rapidly evolving toward serving goals broader than privacy to help innovate and drive businesses forward by smartly managing data. Expect new roles that did not exist (like Data Strategy and Policy Officer in corporate or Practice Innovation Officer in Am Law) to continue to evolve and become available. For many, these will be new roles, without predecessors, some hired from within, others externally.

Another possible disruption to the current state of the privacy market would be the emergence of a dominant software technology that forces talent proliferation of skills in that technology. While many would argue that the core principles of privacy are tool-agnostic, professionals in the e-discovery vertical (for example) might argue the same; however, in the e-discovery war for the talent, one dominant software — Relativity — plays a key role in how hiring managers hire and assess talent. Right now, IAPP certifications hold a similar dominance and credibility for privacy hiring managers, but in no way are they tool-specific in training and education. **According to the IAPP:** “Nearly one in three privacy professionals holds a CIPP/E certification from the IAPP, up a remarkable 11% from 2017.” While a “silver bullet” technology is not likely to replace the necessary frameworks surrounding what is considered essential privacy skill sets, it is possible a tool may become so prevalent in this market that hiring managers begin looking for plug-and-play talent that can wield that technology for instant augmentation. No one predicted that would happen in e-discovery, but it did, and it remains a primary hiring protocol.

Final Thoughts

The privacy profession is just getting started. Expect the evolution of seasoned privacy talent and their matriculation into tertiary fields like data governance, security, risk, or policy to create room for vertical growth of incumbents across the privacy ecosystem who hold official or unofficial deputy-like titles. Expect most staffing to occur in the middle of the market, with semi-seasoned privacy professionals with three to seven years' experience, lawyers or not, to be highly desired and earning between \$100 and \$200K base compensation annually, depending on the role. Expect technology skill sets to play an increasingly important role in how hiring managers evaluate privacy talent, especially for the higher paid and harder to fill privacy engineer roles. Expect professionals who do some privacy work in their current role to shift focus to become fully-fledged privacy pros! Expect the future state of the U.S. privacy job market to be healthy and hearty.



Rachael Haher

Business Development Manager

TRU Staffing Partners

P: 718-541-3630

E: rachael@trustaffingpartners.com