PAUL HASTINGS

PH PERSPECTIVES

September 2019

Follow @Paul_Hastings

The Path Ahead: With Scope of CCPA in Flux, Employers Consider Privacy Implications of New Tech

By Ryan Derry, Anna Skaggs & Jeffrey Wohl

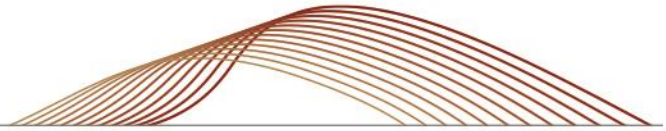
Advances in technology present new opportunities for increased efficiencies, including in the areas of applicant screening and hiring, retention, and incentivizing employee performance. However, these advances also implicate important questions regarding privacy. Employers, individuals and government all are grappling with what information can be collected, whether it should be collected, and its potential and permissible uses if and when collected.

To discuss these emerging issues, against the backdrop of the California Consumer Privacy Act ("CCPA") and other recent privacy statutes, on June 21, 2019, the Employment Law Department of Paul Hastings sponsored a panel titled "Dispersion of Work – Employee Data." The panel was moderated by Ryan Derry and Jeffrey Wohl, partners in Paul Hastings's San Francisco office, and included panelists Ernest Ng, VP of Global Employee Success Strategy and People Analytics at Salesforce, and Ari Waldman, Professor of Law and Director of the Innovation Center for Law and Technology at New York Law School.

Current Status of the CCPA

Any discussion of employee privacy within California must recognize the CCPA and uncertainty about its application to California employers. In June 2018, California adopted the CCPA, a comprehensive privacy statute that has been characterized as California's version of the European Union's General Data Protection Regulation ("GDPR"). The CCPA, which takes effect on January 1, 2020, creates a private right of action and five primary rights for California residents: (1) notice as to what personal information is being collected about them and how it is being used; (2) access to the specific personal information collected, among other things; (3) the ability to opt out of the sale of their personal information; (4) the ability to request deletion of their information, subject to some exceptions; and (5) against discrimination for exercising their rights under the CCPA.

As presently chaptered, the CCPA covers a broad range of employment-related data in light of its definitions of "consumer" ("a natural person who is a California resident"), "business" (any legal entity that does business in California and has annual gross revenues over $25 million), and "personal information" (including "professional or employment-related information" and "educational information").



That may change. In May 2019, the California Assembly unanimously passed AB 25, which would drastically narrow the CCPA's scope by removing employees from the definition of "consumer" and exempting employers from many of the law's requirements. In July, however, the California Senate's Judiciary Committee proposed a weaker version of the bill. In part, the committee's proposal would carve out the CCPA's rights of access, opt-out, and deletion—but not of notice—for employees and applicants. More significantly, the proposed bill contains a sunset provision under which the exception for employees and applicants would expire on January 1, 2021. In other words, the bill would provide employers only temporary relief, and would set the stage for continued dialogue on employee data privacy in 2020.

At this point, the future of AB 25 is uncertain. It remains in committee in the Senate. If it passes the full Senate, the two houses will need to reconcile the differences between the Assembly and Senate versions and send the final legislation to Governor Newsom before they adjourn on September 13. If the bill is not signed into law, the CCPA will apply in full to applicant and employee data effective January 1, 2020.

Accordingly, employers should be ready to comply with the CCPA if the law comes into effect on January 1.

A few open questions to consider:

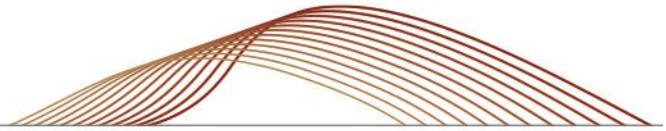
- The current draft of AB 25 would require employers to provide notice of the categories of personal information they collect from individuals and the purpose for which they will use it. It is unclear, however, whether a broadly drafted notice at the beginning of the application process or employment relationship will suffice, or if employers must provide additional notice for every additional category of information they decide to collect.

- Under the CCPA, "personal information" extends well beyond identifying and contact information. Where permitted by law, it includes information related to an individual's health, finances, hours worked, wages paid, performance, and discipline. What the CCPA does not address is whether personal information also includes notes prepared about an applicant during his or her interview, a manager's files on an employee, or other categories of information that employers typically would not disclose to employees.

- Employers may not discriminate against an applicant or employee for exercising his or her rights under the CCPA. However, the CCPA does not restrict an employer's right to comply with the law or judicial process seeking personal information or to prosecute or defend against legal claims. Aside from functioning as a general "savings clause," it remains to be seen what this means for employers in terms of compliance with the CCPA.

Employee Privacy in the Digital Age: Risks and Rewards

As panelists observed, the CCPA can be seen as a reaction to advances in technology made possible by the aggregation of personal data, including employment-related data. Indeed, as artificial intelligence ("AI") has advanced, so have data-driven approaches to employment decisions traditionally made by humans. For example, there has been increasing investment in AI for recruitment and hiring, including scraping of social media platforms, linguistic analysis of writing samples, and game-based assessments. The goal: to predict cognitive ability, personality, communication skills, stress-tolerance, leadership potential, and other desirable—and not so desirable—traits. We have also seen a rise in the use of AI to make predictions about current



employees, such as who is likely to leave the company, who is ready for promotion, and even what benefits an employer should offer.

Employers can leverage these technologies to recruit top performers, help them thrive, and prevent attrition. However, these technologies also raise a host of questions about accuracy, bias, legality, data privacy, and employee trust.

Among other issues panelists discussed is one at the forefront of employee privacy: the expanding role of biometrics. In a spirited debate, panelists assessed the pros and cons of using facial- and voice-recognition software in the interview process. On the one hand, the panel observed, micro-expressions and changes in pitch that are virtually undetectable to humans can be reliable indicia of behaviors like dishonesty, making this software a promising solution to eliminate potential human error and bias. On the other hand, such technology has the potential to create disparate impact, and it is only as valid as the aggregated data it relies upon. Complicating matters, the GDPR requires employers with European Union-based employees to provide "meaningful information" about the logic involved in any automated decision-making, and many of these algorithms are proprietary black boxes.

Deciding When and How to Leverage AI

In light of the questions presented—not to mention uncertainty regarding public acceptance of the use of certain technologies—it is critical for employers to consider how they can leverage machine learning in a productive and beneficial way. For example, as one panelist discussed, AI-supported models for predicting resignations are not necessarily more accurate or useful than traditional models that rely on decades of behavioral research in the area of employee retention.

One panelist suggested a framework in which an employer evaluates the benefit proposition from the perspective of its employees: *What is the employer trying to accomplish? What personal data does the employer need to collect? How will it use the data? How do employees benefit from the collection of this data? Why should employees trust the collection of the data?* And, perhaps a culmination of these questions: *Is there a less invasive way to achieve the desired result?*

Conclusion

These and other important questions facing employers are at the core of the Future of Work, and Paul Hastings is equipped to advise. Please contact Paul Hastings's Employment Law Department to learn more.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings San Francisco lawyers:

Ryan D. Derry
1.415.856.7092
ryanderry@paulhastings.com

Jeffrey D. Wohl
1.415.856.7255
jeffwohl@paulhastings.com