As companies brace for the impact of COVID-19, the last thing on everyone’s mind may be proactive privacy compliance obligations. Certainly, companies may be thinking about privacy obligations that relate specifically to their COVID-19 response. What types of employee information can be disclosed, for example, especially in European offices? (On this, see guidance from the French, Italian and Irish data protection authorities.) But companies can think more broadly, in particular about how they will continue the proactive operations of the privacy team during this time. Some questions companies can ask themselves now include:

- How will employees continue to fulfill CCPA and GDPR rights requests if the work force is remote?

- How are privacy functions ensuring that personal information is being used in compliant ways? For example, when companies turn to technologies to facilitate remote communications, like texts, which are governed by TCPA discussed in more detail here, are organizations sufficiently knowledgeable about those laws’ requirements?

- Or, if companies move to using biometric-based, touch-free entry systems to limit the spread of germs, is there a strong understanding of the legal requirements? (The use of these technologies being regulated in many states, as we have discussed in the past.)

- What about companies considering using geographic tracking systems to help locate employees? These activities, too, are often
In addition to new activities that might impact existing laws, many jurisdictions are proposing new privacy regulations (as we have written previously), which appear to be moving forward despite COVID-19. Add to this that several existing privacy laws have private rights of action, and there may be actions brought under those laws in the coming months despite COVID-19. All of this collectively points to an increase in demand for the privacy function’s time.

Typically when demand increases, teams meet to brainstorm through in-person meetings or off-site retreats. And, under normal business circumstances, companies facing these pressures (new laws, potential privacy-based law suits) include in compliance efforts data diligence exercises. These help companies get a good handle on what data they have, how they obtained it, and how it is being used. Normally - as with brainstorming - the emphasis is on in-person data gathering, allowing fulsome conversations that go beyond questionnaires. The results of these efforts help companies understand the scope of their privacy obligations, design compliance programs, and implement those programs.

In light of the new business environment under COVID-19, many may be concerned about how to conduct planning and diligence efforts if key personnel are working remotely and travel is restricted. Instead of deferring important planning and diligence exercises, companies can turn to interactive virtual platforms, and make good use of the interactive features of those platforms – like communicating with cameras (and having cameras turned on). Using these tools, teams can use this time to not only ensure ongoing compliance in this business climate, but also to get ahead of upcoming privacy regulations.

**Putting it Into Practice:** Privacy teams may want to take the opportunity now to get ahead of the potential uptick in individuals making rights requests, new methods of data use by business teams, and upcoming privacy laws.

Copyright © 2020, Sheppard Mullin Richter & Hampton LLP.