VLP Partner Michael Whitener Interviewed by Inside Counsel in the Article “The Employee Privacy Risks of Company Chips”

VLP Partner Michael Whitener sat down with *Inside Counsel* magazine to discuss the risks associated with company microchips, including employee privacy, data collection policies and data misuse–and even hacking.

The article, “The Employee Privacy Risks of Company Chips,” reported on a software company that has a new voluntary program to employees, where a microchip is implanted in their hand. The chip then allows the employees to open doors, pay for purchases, share business cards, store medical information, and even log into their computers. The article noted that, although the chip is making certain tasks easier for people, it could also be creating serious privacy risks.

Mr. Whitener noted, however, that these privacy risks are no different than the risk of someone stealing a wallet containing credit card information or hacking someone’s passwords. “The fact that the information is contained in an implanted chip, rather than on a plastic card or other media, isn’t material from a privacy perspective. In fact, one could make a case that an implanted chip is more secure,” he said.

According to the article, the real risk is that implantable devices might become a job requirement and expand beyond a convenience for employees.

“Of course, the ‘creepy factor’ is high when it comes to implanted devices–it calls to mind movies that portray dystopian surveillance societies, including ‘Gattaca’ and ‘Minority Report,’” Mr. Whitener explained. But he noted that there is nothing about this company’s program itself to justify those concerns because the microchip doesn’t have tracking capabilities.

Click here to view the entire article.