With a background in computer programming and an interest in national security, Beth George was an ideal candidate to manage the legal implications of cyberattacks on the U.S. government. Her skills were quickly put to the test by two of the largest breaches the government had ever experienced. Now, in Silicon Valley, George helps clients avoid the fate that befell the government. Working with "hypertechnical" clients, George emphasizes the importance of cybersecurity "not merely because they're connected to the internet but because their entire product is based on internet connectivity."

Not long after George joined the White House counsel's office, a government contractor named Edward Snowden leaked highly sensitive data on intelligence gathering by the National Security Agency. George was assigned to advise the U.S. Senate Select Committee on Intelligence in its review of Snowden's disclosures. Then, in 2015, George was the White House's lead associate counsel on a data breach at the Office of Personnel Management, which exposed confidential data on current and former federal workers, including many with high-level security clearances. George helped agencies identify and secure their most important and vulnerable digital assets — within 30 days. "There really was a call to action on governance of that issue."

When she left the government in 2017, George wanted to build a cybersecurity practice on the West Coast amid the tech giants whose security and privacy policies had begun receiving intense scrutiny from regulators and consumers alike. George advises clients to think and act proactively: "What are we doing now and how can we be in front of the next questions about privacy and security — not only how do we comply with the laws as they are written today, but how are we making ourselves leaders in the field?"