The New State of Data Privacy:
## Q&A With Michelle Finneran Dennedy of Privatus Strategic Consulting & CEO, PrivacyCode, Inc.

The Privacy Tech landscape is both evolving and expanding, with private companies taking on new roles and responsibilities and making new investments in the consumer privacy space. The number of privacy tech companies has increased roughly 8X since 2016. Wishing to better understand this "new state of data privacy," we turned to a longtime expert in the space and interviewed Michelle Dennedy, the former Chief Privacy Officer of Cisco, McAfee, and Sun Microsystems who is currently a Partner at Privatus Strategic Consulting. You can follow her on Twitter at @mdennedy.

How do you think the landscape of the "new state of data privacy" currently looks with regard to the roles, responsibilities, and investment that private companies are making in the consumer privacy space?

"Privacy engineering" for privacy outcomes has never been more important to business outcomes. The roles that previously may have been limited to data security, identity management, and legal specialties have exploded into every part of the enterprise: data officers, technical teams, financial evaluation, and risk governance teams all must have a hands-on view on how to operationalize, measure and build privacy outcomes throughout data lifecycles. The privacy engineer must be able to get down to the granular control levels, have a working knowledge of data science capabilities, and be able to communicate up through senior management.

What is "privacy-as-a-product" in your opinion? Is that a good space to build products in or invest in? Why or why not?

As a CEO and builder in this space, I may be a bit biased. As a multi-decade veteran building and leading privacy, sales, policy and cloud teams in the privacy space, I want a privacy product, privacy enhancing technology component and a privacy engineering platform and I want it NOW. Chief Privacy Officers can no longer live on spreadsheets alone; we cannot trust online survey tools to have the deep accuracy we need; we must have metrics to create, test and update objectives and key results.
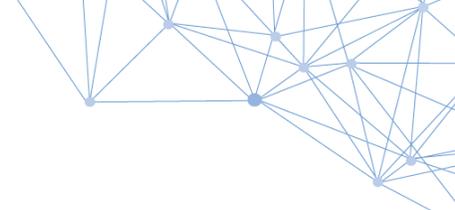
So, yes we need privacy-as-a-product. We need privacy outcomes – even those that include sensitive personal data – that are governed, processed and managed according to moral, ethical, legal and sustainable requirements. So-called "virtual" or Web3 environments are becoming a key part of sustainable economic stability; Health and education services must traverse an in person and online lifeline to drive better outcomes for individual people while creating economic opportunity and innovation. Even traditional brick-and-mortar goods and services businesses are dependent on data to increase value creation. Every business that has customers or employees requires privacy orchestration and the tools to make every data-related or recorded activity safe and valuable.

There's a technology startup based in Charleston, SC in the privacy and education space, [Data Protocol](#), that is training software developers in better data privacy practices. What do you think about what they're doing?

I am thrilled that there are dedicated companies like Data Protocol that are enabling privacy engineers to add to their skill sets and giving other technical professionals a way into the world of privacy engineering. Education in this discipline opens the door to an explosion of meaningful and growing career paths.

What's the next stage of privacy-as-a-product? Where is this space going, and what are the roles of big and small companies vs. the government or nonprofit bodies?

There is an entire tech stack growing and evolving to meet the complex challenges that arise in the data governance and privacy space. The range will continue to span the post-production compliance checklist and workflow packages, inventory tracing and availability, privacy-enhancing tech such as masking, anonymization, segmentation, encryption, etc., and platforms like [PrivacyCode](#) that shift all the way left to the earliest stages of design and change management. There will be specialties that govern a deeply personal one-to-one interaction such as a communication between legal counsel and client; there will be hundreds of new ad-tech pods and vaults and fuzzing that allow companies to get in front of buyers without intrusive and unethical surveillance methods.

In short, the innovation in Privacy Tech will be as varied and specialized and valuable as our human interactions are. Privacy is, after all, functionally defined as the authorized processing from cradle to grave according to moral, ethical and sustainable principles. Start your imaginations & build!
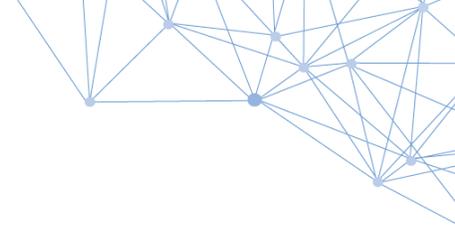
This is the first in a Q&A series that DCI will be publishing on the topic of Privacy Tech to better inform and engage policy and business stakeholders who are both influencing and influenced by these new dynamics in the privacy landscape.