S		
ecurity versus surveillance—what’s the difference? And how can we—IT staff and leaders—engage the campus community in a security and privacy discussion that supports different points of view on technology choices so that we can take advantage of the opportunities to secure the campus environment and protect privacy? New technologies offer new capabilities, but they also have the potential to create controversy on campus. How can we ensure that security and privacy reinforce, rather than wrestle against, each other? We have the ability, now more than ever, to be extremely proactive to ensure that our students, faculty, and staff have amazing—and secure—learning, education, and research services. Are we doing enough to protect our community, or are there opportunities to do more?

When we reflect on the primary goals of higher education, student success is undoubtedly a key pillar. In fact, some might even go so far as to say it defines the very reason for the college/university’s existence. Enabling student success includes leveraging technology to build robust communities, provide high-quality services that deliver a top-notch learning experience, and protect our students during their time at our institution in a way that meets today’s rapidly evolving security and privacy expectations.

What’s stopping us from rapidly delivering increasingly relevant services to meet our institutional goals? I’d like to challenge our line of thinking and have us consider whether it’s time for a course correction. Are we envisioning alignment between privacy and security (rather than a collision course), proactively addressing threats entering our domain (rather than passively standing by or, worse yet, surveilling), and leveraging technology to integrate for a seamless and safe experience? If we aren’t quite sure the answer is yes, let’s explore for a moment how we might go about this differently.

With significant technology advancements in recent years, we have increasing capacities to collect and store data at rates nearly unthinkable only a few short years ago. In fact, Statista predicts that by the end of 2019, we will have 26.66 billion internet-connected devices across the globe.¹ These solutions, combined with the power of our enterprise service capabilities, afford greater opportunities to streamline and simplify the education and research experience, moving well beyond wayfinding to collaboration with friends and to event suggestions provided via a voice-enabled campus technology, all while offering increasingly improved services to protect our students so that they can focus on their education.

Why aren’t we leveraging these capabilities to deploy services more quickly? For one thing, there is more than a little work involved in bringing these solutions in, as we push the boundaries of today’s service capabilities while at the same time ensure that each new initiative doesn’t upset the delicate balance of operational activities or risk acceptance. But let’s envision a world where we speed up our deployments, taking us from where we are now to third, fourth, or ultimately fifth gear. Let’s lean in to the technical advances of the last decade and incorporate intelligent observation to ensure we aren’t simply moving to a data-collection model that may serve more to surveil our communities than to actively protect them.

How could we improve? First, all of our teams should be focused on delivering services that meet both

¹ Source: Statista
In a world that is increasingly defined by data and information, those of us in higher education information technology must question our assumptions about security and privacy as we move forward. Above all else, we must listen to our students, faculty, and staff and foster a community of raving fans.

- **Building trust in our community** means that we are transparent in the services we provide and how we leverage the data. In a world where there is a tendency to collect more data than we need, keep it for longer than we should, and react to security breaches rather than proactively combating the threat, it is increasingly important for us to communicate early and often. Managing data responsibly requires that we clearly articulate the uses for data collection and that we store data only as long as it is needed to provide a service.

- **Designing with privacy in mind** consists of considering the protection of personal data during each step of the development, design, selection, and use of IT services and systems. Creating this culture within our organizations is essential.

- **Embedding security in our development initiatives** requires that proactive security is a fundamental principle for which each of us—not just one individual or one small team—is responsible.

- **Integrating and automating** removes manual processes and frees up staff for higher-value work.

- **Moving quickly** by creating a vibrant Development/Security/Operations (DEV/SEC/OPS) culture with a bias toward action helps us lean in to the agile mindset.

At ASU we proactively seek opportunities to embed these concepts into our design principles. We embed security analysts and architects with cloud development teams, investing in security tools to aid development efforts and organically producing increasingly security-focused development. The result is rapid deployment of new application features with significantly more robust security from the start. ASU has taken a similar approach to meet transparency and privacy concerns: the security office has instituted a governance structure in conjunction with the provost’s office to elevate privacy discussions and decision-making involving stakeholders and executive leaders from across university departments and units. This action has resulted in a collaborative and high-functioning ASU privacy team. Continuing with our theme of being deeply embedded, ASU has a long-standing culture of empowering staff to buy enterprise solutions where well-established commercial solutions exist, thus freeing up staff time to focus on creative efforts to build innovative solutions to meet the various needs of our community. In a specific use case related to the constant barrage of cyberthreats, for example, we’ve constructed a set of fully automated email, firewall, and identity solutions that leverage robust threat intelligence to take immediate action to protect the university from external attacks, again freeing up staff to focus on higher-value initiatives.

Let us challenge ourselves and our IT teams to tackle this paradigm shift, building trust through meaningful transparency, thinking about privacy first, embedding proactive security in everything we do, integrating systems to remove repetitive tasks, and removing barriers that keep us from moving quickly. Let’s dream big and take time to imagine the “art of the possible.”

In a world that is increasingly defined by data and information, those of us in higher education information technology must question our assumptions about security and privacy as we move forward. Above all else, we must listen to our students, faculty, and staff and foster a community of raving fans.

**Note**


Tina Thorstenson (Tina.Thorstenson@asu.edu) is Deputy CIO for IT Governance, Policy, and Information Security at Arizona State University and also continues to serve as Chief Information Security Officer, a position she assumed in September 2009.