Tech industry seeks new frontiers as Congress lags behind
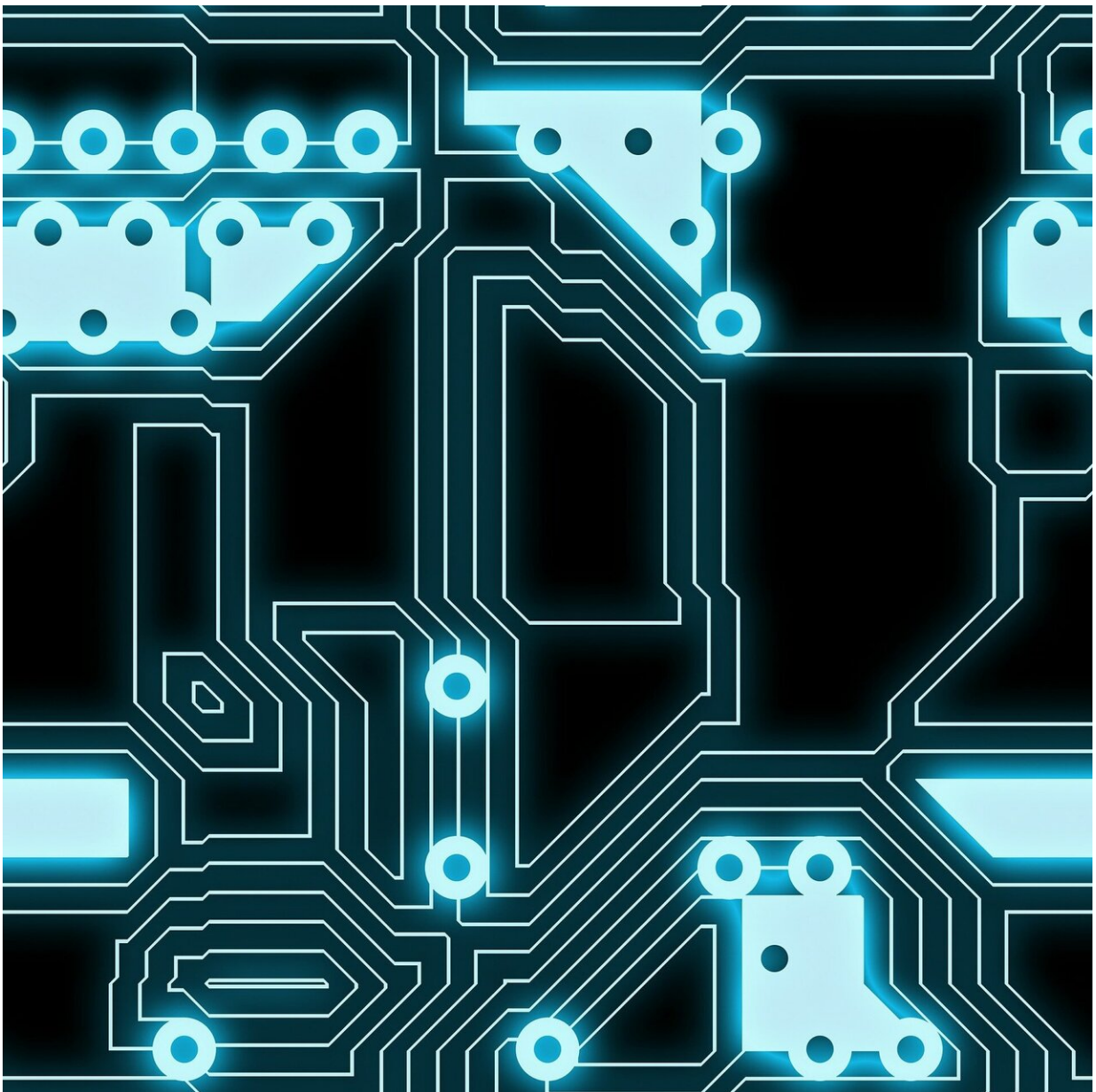
February 2 2022, by Gopal Ratnam

Tech companies are racing toward new frontiers involving immersive virtual reality worlds that some experts fear could exacerbate existing problems as Congress lags behind the sector's rapid developments.

The emerging technologies will further test lawmakers, who are still grappling with addressing tech-enabled dangers such as online misinformation and disinformation, data theft and loss of privacy that plague people's computers and smartphones.

Facebook and Instagram parent Meta, Microsoft, graphics processing company Nvidia and game platform company Roblox are among the major tech companies that are working to build the metaverse, a term first coined by Neal Stephenson in his science fiction novel "Snow Crash." The term refers to shared, virtual worlds that parallel the real world.

Donning headsets such as Meta's Oculus or Microsoft's HoloLens, users can immerse themselves in virtual reality worlds that mimic or extend the physical world.

Security experts and some governments around the world worry that without adequate safeguards, today's online dangers could spread to the new virtual worlds.

"As soon as you connect people" on virtual reality platforms, "you bring in all those traditional risks like moderation, harassment, bullying, the plethora of disinformation, misinformation," said Kavya Pearlman, a security researcher and founder of XR Safety Initiative, a nonprofit group that promotes safety in virtual reality worlds.

Virtual worlds would enable virtual economies where users spend money to create and maintain their avatars or buy virtual goods and services, all of which would pose new problems involving cryptocurrencies or custom currencies that the creators of virtual worlds might create, Pearlman said.

Virtual reality advertisers could likely track users' eye movements in order to place digital billboards that are in the center of one's vision instead of on the periphery, said Jon Callas, a cryptographer and projects director at the Electronic Frontier Foundation.

Australia's eSafety Commissioner has said while immersive virtual technologies would likely transform education, health care, entertainment and military applications, they also are likely to pose new risks.

"By providing hyper-realistic experiences—where virtual sensations feel real—immersive technologies could increase the impact of negative interactions, and lead to a rise in online assaults and abuse," the Australian eSafety Commissioner said in a position statement on its website.

Meta CEO Mark Zuckerberg and Vasu Jakkal, Microsoft's corporate vice president for security and compliance, have said their companies intend to develop the new technologies with consumer privacy and safety in mind.

Jakkal has said the metaverse is likely to lead to an "explosion of devices … apps and data." He told the publication Venture Beat recently that the increase in apps, devices and underlying infrastructure means "it's just increased your attack surface by an order of magnitude."

The technologies underlying the metaverse are still in development and

there should be a balance between "regulating and over-regulating to the point where emerging technologies are stifled," said Joan O'Hara, vice president for public policy at the XR Association, an industry group that represents Meta, Microsoft, Google, Sony and others.

Unlike the previous generation of technologies, when the tech industry began engaging with Congress only after evidence of privacy invasion and disinformation campaigns had done damage, companies are now engaging lawmakers during metaverse development, so "that's a positive," O'Hara said.

While Congress has addressed children's online privacy and online pornography, it has yet to pass legislation to address data privacy, or the spread of disinformation and misinformation.

Congress, the federal government and operators of critical infrastructure are still struggling to plug security gaps and contain devastating cyberattacks that have crippled fuel supplies and shut down government agencies, Fortune 100 companies and school systems.

Several data privacy legislative proposals that have been debated over the past four years but have yet to become law would apply protections in the context of emerging technologies, said Aaron Cooper, vice president of global policy at the BSA Software Alliance.

At their core, Cooper said, those bills address two key elements: "One is making sure consumers have rights over their data. And the other is making sure that companies act responsibly with their data and not in a way that would be counter to what their customers would expect."

Congress also should consider laws addressing biometric security, Callas said, pointing to such an Illinois state law.

The Illinois legislature in 2008 passed the Biometric Privacy Information Act, which prohibits companies from collecting biometric information like fingerprints, iris scans, facial geometry, voice identification and DNA without the explicit consent of users.

It may take close to another decade before the 3D metaverse envisioned by tech titans takes shape fully—but even then it is unlikely users will abandon 2D devices like laptops and smartphones, Callas said.

"It's not as if we are going to suddenly stop reading news articles on a 2D screen and switch to a headset," Callas said. Just as smartphones did not replace laptops but became an additional device, metaverse devices are likely to stand on their own.