Gen™

2025

U.S. Digital and Cyber Policy Issues:

Overview and Recommendations

norton™ Avast™ LifeLock™ by norton MoneyLion®

With the new administration in Washington, DC, shifts in U.S. tech policy are anticipated, driven by new leadership at federal agencies, evolving political priorities, and a rapidly changing technological landscape. This document outlines key policy areas — consumer protection and online safety, the cybersecurity skills gap, generative AI and consumer privacy — and suggests how legislators can craft public policy that protects digital freedom for the future.

Focus on Consumer Protection Against Online Scams and Cybercrime

Consumers should have the freedom to choose their cybersecurity provider and monitor their full digital experience on desktop, mobile and in the cloud, and people should be able to safely and confidently engage in the digital economy. This choice empowers people to defend against scams and malware, shifting control from providers to the individual, and fostering a more secure digital environment.

Consumer freedom to choose cybersecurity providers allows access to monitor their operating system, websites, apps, and software, while empowering them to make decisions about how they make their digital environment secure. Some Operating System developers restrict cybersecurity solutions from accessing key system components. The loss of access to these control points not only creates competition issues but, more importantly, it exposes consumers to cybersecurity risks by limiting their use of the cybersecurity products they've chosen.

The debate around consumer digital security also extends to online platforms, including social networks, messaging applications and in the future metaverse. Given that most scams, particularly AI-based ones, are disseminated through these platforms, Gen believes that third-party cybersecurity providers should have access to online platforms to increase consumer protection against cybersecurity threats.

Recommendations

- Create an opportunity for digital platforms, operating systems and digital service providers to offer options including third-party antivirus and cybersecurity solution providers during the initial setup or installation process of devices. This promotes consumer choice and awareness.
- Encourage competition among digital platforms, operating systems, and digital services providers to ensure that their products are designed and developed to enable seamless integration and compatibility with a wide array of third-party anti-malware, anti-scam, anti-fraud and other cybersecurity solutions.

Champion Child Online Safety

Ensuring online child safety is a crucial issue that requires a multifaceted approach. While access to technology is vital for youth to learn, connect and expand their world to our interconnected global society, bad actors seek to violate their safety and privacy.

Gen provides Cyber Safety education, training, and product donations that support young people to stay safe online. We have reached over 5.3 million people through our Cyber Safety education and training, made possible through a range of programs that bring together our unique expertise, our consumer brands and external partners. For example, Gen backs the Save the Children's "Creating a Safe and Enabling Experience for Children Online" program, which provides online safety education to children across India. Through this program, we have increased parents' and teachers' awareness of the risks of exposing children to the internet, with training sessions for teachers completed in 50 schools.

Recommendations

- Foster collaboration between legislative and regulating bodies, tech companies and non-profit organizations to develop and implement technologies and frameworks that enhance the online safety of children.
- Strengthen data privacy laws to protect children's personal information from being collected and misused by platforms.
- Implement awareness campaigns for children, parents/guardians and educators to help them identify and report inappropriate and harmful content and interactions.
- Promote clear and accessible reporting mechanisms for children, parents/guardians and educators, like the National Center for Missing & Exploited Children's tip line.

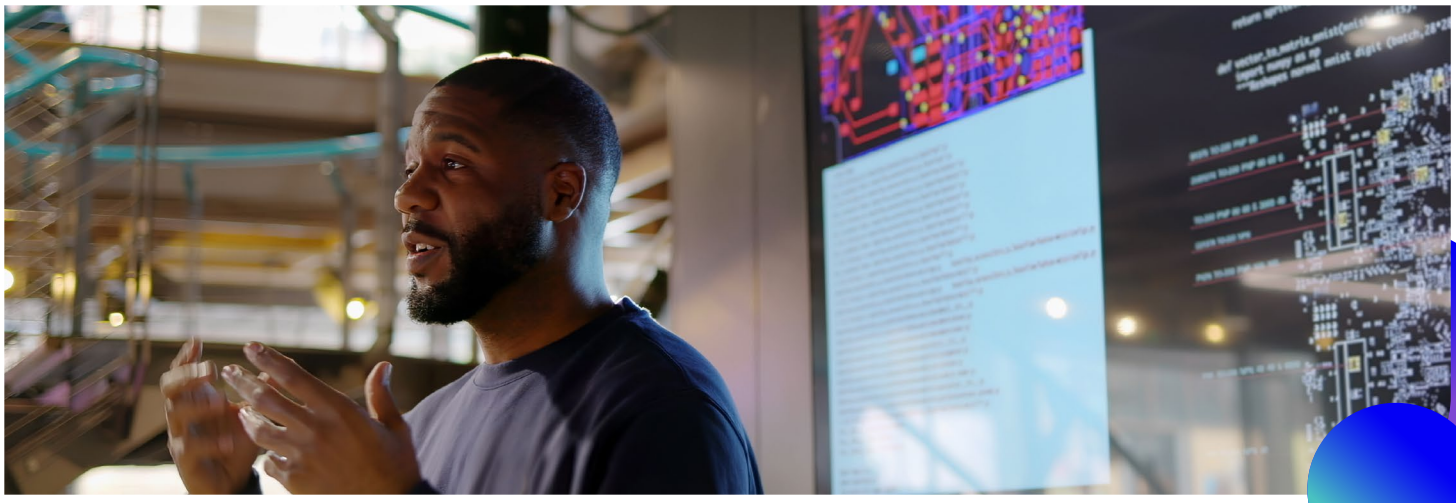
Foster Cybereducation

The recent surge in cybercrime, including scams, phishing and malvertising, demonstrates the urgent need for enhanced skills and awareness in the cybersecurity field. This dire situation underscores the necessity for comprehensive education and a push for cybersecurity competence for a diverse range of professionals.

Gen blocked 10 billion attacks in 2023, a 49% increase year-over-year. And of those threats, more than 75% of all threat detections on desktops were attributed to scams, phishing and malvertising.

Recommendations

- Launch comprehensive literacy programs to educate the public on basic and evolving cybersecurity principles, the risks associated with cybercrime, and the steps individuals can take to protect themselves online.
- Foster public-private partnerships to develop and deliver cybersecurity training programs, leveraging the expertise and resources from both sectors to improve cyber literacy and skills.
- Encourage companies to invest in cybersecurity training for their employees.



Leveraging Artificial Intelligence to Fight Cybercrime

The size of the artificial intelligence market in the United States is estimated to reach 223.68 billion USD and reach a peak by 2030. As generative AI grows and becomes more sophisticated, so do the threats that come along with it. Cybercriminals are leveraging AI at an unacceptable level to disseminate deceptive messaging, deepfakes, and malicious content. It is vital that we safeguard against misuse of AI-generated data, in order to help protect consumers.

While personalized online experiences offer significant value to consumers, some uses can also present major societal threats, particularly in the context of generative AI. Because extensive data collection can be needed for personalization, this can lead to privacy concerns. Another potential risk is biases in AI algorithms that can lead to unfair or discriminatory outcomes.

Our commitment to privacy is foundational. And our customer-first approach ensures personal data is processed with the utmost respect for privacy. Gen processes data in a manner aligned with the expectations of our customers and strives for maximum transparency. We encourage consumers to safeguard their online presence and use effective privacy measures.

Recommendations

- Encourage citizens to only use intelligent chatbots and generative models from providers who offer clear legal guarantees against the misuse of private data.
- Recommend companies to increase transparency about training data, risks, and analysis on the potential for abuse or errors.
- Support measures that aim to raise public awareness regarding the issue of content authenticity on the Internet and provide tools to ensure that AI bots are distinguishable from real people.
- Promote legislative efforts to require online platforms and service providers to promote client-side recommendations, personalization transparency, and third-party personalization control and explainability technology.
- Advocate for policies that bolster individuals' control over their data, facilitating easy management, retrieval or deletion of personal data.
- Focus on promoting transparency in the processing of personal data.

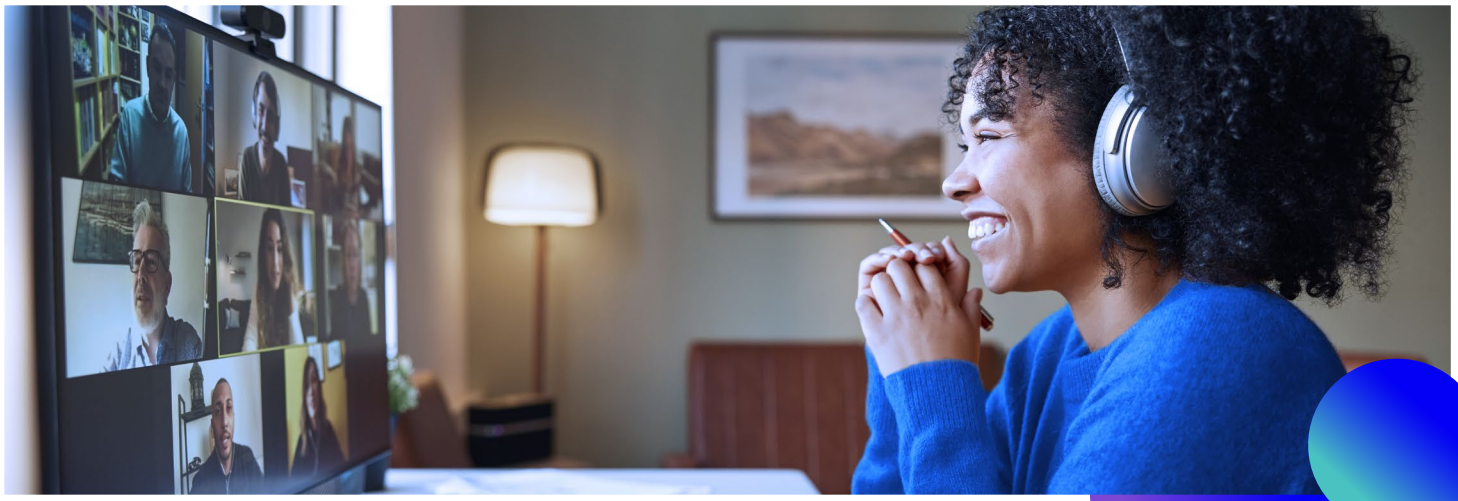
Promote Interoperability in Digital Identity

The average individual manages over 150 online accounts, with personal data scattered across numerous databases globally. The escalating trend of data breaches amplifies the threat of identity fraud. Individual privacy and security should not be compromised to access more online services. Intuitive, cross-platform solutions can empower individuals to manage their data and identity more seamlessly and easier. For instance, Generative Adversarial Networks (GANs) work to secure digital identities by improving face recognition, preventing fraud, and protecting user privacy. GANs generate realistic but false data to train better ID systems, making online verification safer, faster and more reliable.

The cornerstone of digital freedom lies in open standard digital wallets, facilitating seamless transactions and management of trusted digital relationships across popular platforms, free from vendor lock-ins. As a founding member of the OpenWallet Foundation (OWF), Gen is a pioneer in the movement towards open-source, interoperable digital wallets.

Recommendations

- Adopt policies that promote user control, data minimization, and privacy-preserving data reusability, and build on learnings from the EU case (eIDAS 2.0).
- Support collaborative efforts like the OpenWallet Foundation and Ayra Association, launched by Gen, that are driving the global acceptance of verifiable credentials and digital wallets, while putting in place the governance and guardrails to protect all parties involved.
- Establish a recommended digital identity framework to enhance security, privacy and accessibility in digital transactions and ensure consumers can instantly recognize organizations that adhere to this framework.



About Gen

Gen is a global company with headquarters in Tempe, Arizona and Prague, Czech Republic. Gen brings award-winning products and services in cybersecurity, online privacy, identity protection and financial wellness to nearly 500 million users in more than 150 countries.

We are dedicated to powering Digital Freedom through our portfolio of trusted consumer brands including Norton, Avast, LifeLock, MoneyLion and more. The Gen family of consumer brands is rooted in providing financial empowerment and cyber safety for the first digital generations. This goes beyond our mission to create innovative and easy-to-use technology solutions that help people grow, manage, and secure their digital and financial lives. Today, we empower people to live their digital lives safely, privately and confidently for generations to come. That's why Gen approaches everything we do with the customers and communities we serve in mind.

If you want more information, please reach-out to:

Kim Allman
Head of Corporate Responsibility,
ESG & Government Affairs
Kim.Allman@GenDigital.com

United States: 60 E Rio Salado Pkwy STE 1000 Tempe, AZ 85203
Czech Republic: Enterprise Office Center Pikrtova 1737/1A 140 00 Prague 4