IEEE★USA IEEE

28 February 2023

Representative Cathy McMorris Rodgers, Chair
House Committee on Energy and Commerce
Washington, DC 20515

Representative Frank Pallone, Jr., Ranking Member
House Committee on Energy and Commerce
Washington, DC 20515

Representative Gus Bilirakis, Chair
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
Washington, DC 20515

Representative Jan Schakowsky, Ranking Member
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
Washington, DC 20515

Dear Rep. McMorris Rodgers, Pallone, Bilirakis, and Schakowsky,

Thank you for conducting the Subcommittee's March 1st hearing on the role of standards in protecting the online privacy of Americans, in particular children. IEEE, as a leading global standards developer, believes that the standardization process is important to both promoting innovation and, as rapidly growing technologies change the way we interact and expose our personal data, ensuring that technologies do not harm users.

The U.S. has for decades consistently, and in our opinion appropriately, promoted the principles of consensus-based standards developed in a decentralized direct-participation model. These principles have contributed greatly to advancing U.S. innovations and technological competitiveness. We encourage the federal government to continue to engage actively and effectively with standards setting bodies as a means of strengthening data privacy governance.

The U.S. should lead discussions on global technical standardization and establishment of a national data privacy standard. Below are listed the IEEE standards and related programs that are most relevant to the protection of online privacy, including IEEE 2089™, a standard that establishes a framework for developing age-appropriate digital services for situations where users are children.

IEEE-USA is the American component of the global IEEE (Institute of Electrical and Electronics Engineers), the world's largest technical professional society. We represent technology professionals in all parts of our 21st century technology-based society – from space exploration to biotech, cryptocurrency to power generation. IEEE has more than 150,000 individual members across the United States. The IEEE Standards Association (IEEE SA) is one of the world's largest global standard setting bodies with a catalog of more than 2100 standards and projects, including many at the heart of our modern economy.

If you have any questions, please do not hesitate to contact Erica Wissolik at (202) 530-8347 or e.wissolik@ieee.org.

Sincerely,

Eduardo F Palacio

Eduardo F. Palacio
President

IEEE Standards and Related Information

Name/Title	**Description**	**Link**
IEEE 7002™ Standard for Data Privacy Process	Defines requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data.	https://standards.ieee.org/ieee/7002/6898/ The PDF of this standard is provided at no cost in the IEEE GET Program at https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=93)
IEEE 2410™ Standard for Biometric Privacy	This standard provides for private identity assertion, and includes a formal specification for privacy and biometrics such that a conforming system will meet GDPR, CCPA, BIPA, or HIPAA privacy requirements.	https://standards.ieee.org/ieee/2410/7746/

IEEE P1912 **Standard for Privacy and Security Framework for Consumer Wireless Devices**	This standard project (in development) defines a privacy scale for data that is defined as personal identifiable information, which is collected, retained, processed, or shared on networked edge, fog, or cloud computing devices. This privacy scale will provide input to assessment tools that developers or users of these applications employ to develop, discover, recognize, or implement appropriate privacy settings for the personal data resident on these devices.	https://standards.ieee.org/ieee/1912/10174/
IEEE 2089™ **Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children.**	This standard establishes a framework for developing age-appropriate digital services for situations where users are children. The framework centers around the following key areas: a) recognition that the user is a child, b) considers the capacity and upholds the rights of children, c) offers terms appropriate to children, d) presents information in an age-appropriate way and e) offers a level of validation for service design decisions.	https://standards.ieee.org/ieee/2089/7633/
IEEE P2876™ **Recommended Practice for Inclusion, Dignity and Privacy in Online Gaming.**	This standard project (in development) defines a set of recommended practices for inclusion, dignity, and privacy in online gaming. It includes a descriptive taxonomy to enable clear and concise communication between stakeholders, and a set of best practices designed to help game developers build more inclusive online communities. A reference model defining common concerns, challenges, and remediation methods across all online games is also included.	https://standards.ieee.org/ieee/2876/10184/

IEEE 802E™ Recommended Practice for Privacy Considerations for IEEE 802® Technologies	This recommended practice helps promote a consistent approach by IEEE 802 protocol developers to mitigate privacy threats identified in the specified privacy threat model, and to provide a privacy guideline.	https://standards.ieee.org/ieee/802E/6242/
IEEE P2933™ Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety and Security.	A set of guidelines and standards is necessary to standardize the use of clinical Internet of Things (IoT) devices for precision medicine, data sharing, interoperability, and security, with a goal of improved and measurable healthcare outcomes and protection of patient data. This standard project will establish that framework, with the incorporation of TIPPSS principles. It will encompass wearable device interoperability with healthcare systems such as electronic health records (EHR), electronic medical records (EMR), other clinical IoT devices, hospital devices, and with future devices and connected healthcare systems.	https://standards.ieee.org/ieee/2933/7592/
IEEE 2883-2022™ Standard for Sanitizing Storage	This standard covers methods of sanitizing logical storage and physical storage, as well as providing technology-specific requirements and guidance for the elimination of recorded data.	https://standards.ieee.org/ieee/2883/10277/
IEEE 1619.1-2018™ Standard for Authenticated Encryption with Length Expansion for Storage Devices	This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media.	https://ieeexplore.ieee.org/document/8637991

IEEE 1619.2-2021™ Standard for Wide-Block Encryption for Shared Storage Media	EME2-AES and XCB-AES wide-block encryption with associated data (EAD) modes of the NIST AES block cipher, providing usage guidelines and test vectors, are described.	https://standards.ieee.org/ieee/1619.2/10252/
IEEE 2089™ Standard for an Age Appropriate Digital Services Framework Based on the 5 Rights Principles for Children	This standard establishes a set of processes by which organizations seek to make their services age appropriate. It sets out processes through the life cycle of development, delivery and distribution that will help organizations ask the right relevant questions of their services, identify risks and opportunities by which to make their services age appropriate and take steps to mitigate risk and embed beneficial systems that support increased age appropriate engagement.	https://standards.ieee.org/ieee/2089/7633/
IEEE 2890™ Recommended Practice for Provenance of Indigenous Peoples' Data	This recommended practice details the rules by which the provenance of Indigenous Peoples' data should be described and recorded.	https://standards.ieee.org/ieee/2890/10318/
IEEE SA Industry Connection Program on Cybersecurity for Next Generation Connectivity Systems	A pre-standardization initiative addressing cyber security issues and rethinking architectures to address critical market needs. IEEE SA proposes five architecture principles or baseline realities that will be used to explore new architectures to create more secure and trusted digital platforms: passwords, phishing, data breaches, privacy erosion and surveillance, and misinformation and unverified sources.	https://standards.ieee.org/industry-connections/cyber-security-for-next-generation-connectivity-systems/
IEEE SA Industry Connections Program on Cybersecurity in Agile	A pre-standardization addressing cloud remote access security, including performing a gap analysis of existing	https://standards.ieee.org/industry-connections/cybersecurity-agile-cloud-computing/

Cloud Computing	cloud standards and certifications and evaluating the need for extending them for secured remote access. Emphasizes defense organizations which have more restricted security requirements and may require more restricted security on remote access to their data.	