IEEE-USA

POSITION STATEMENT

Digital Personal Privacy, Awareness, and Control

Adopted by the IEEE-USA Board of Directors November 4, 2021

IEEE-USA supports greatly strengthening laws and regulations protecting individual digital privacy in this era of big data, analytics, and artificial intelligence. The U.S. has fewer restrictions on the collection, use, and possible abuse of personal information than many other countries, including those in the European Union. Advances in information technologies have created situations where U.S. citizens are largely unaware of the extent and scope to which their personal data is being collected, how it is being used, and who is applying that data to influence their, or others', actions. Congress and regulatory agencies should adopt and implement laws, regulations, and processes that significantly increase the digital privacy protections of U.S. citizens.

Threats to Americans' digital privacy abound. Physical identification methods like facial recognition, voice recognition, "smart" devices, and electronic identifiers are used to track individuals. Digital sources, including online data collection, data analytics, compromised communications, and physical identification methods can be used to build a comprehensive picture of an individual. This understanding is then used to identify personal vulnerabilities, manipulate individuals, steal identities, and otherwise exploit or harm individuals, all with little or no disclosure of the collectors' intentions or identity.

IEEE-USA advocates for strong legal protection for individual privacy. Fundamentally, Government policies must recognize that individuals own information collected or inferred about them. Examples of specific areas where increased protections are needed include:

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: https://www.ieeeusa.org

Public Transparency:

- The public must be able to easily learn: the types of data being collected or inferred by any web service, device or other electronic means; what data is retained and for how long; how it is used; and with which third parties it is shared, directly or indirectly. The same information must be available from those third parties.
- All data collection mechanisms and devices must be disclosed to users, including web beacons, GPS location reporting, imaging/cameras, IoT device interactions or other mechanisms for tracking user activity or data. Disclosed information must be sufficient for users to identify and invoke their privacy rights.
- Each web service, or application must disclose ongoing content placed on the user's device and the uses of that content. This also applies to devices connecting to the Internet, or otherwise sharing data collected. Communications, processing or storage of data outside of the United States must be disclosed to users, even if data is not retained on the collecting device(s).
- These disclosures must be readily accessible and comprehensible to the average user without specialized knowledge.

Disclosure for Users:

- For each web service or application, users must be able to obtain complete disclosure of information about them that is retained by the service, application, device or third party accessing the user's information – directly or indirectly.
- Similar disclosure and protections must also apply to third parties able to collect and retain personal data, including disclosure identifying all such third parties.

Control:

- Location and operational information from on-line devices may not be used for commercial purposes without explicit, informed user consent. Specific parameters affecting user contracts, pricing and liability must be provided to users prior to enabling such access.
- Users must be able to remove personally identifiable data about them easily from any site, cloud or collection device.
- Users must be able easily to identify, terminate, delete and/or uninstall any content or applications placed on their devices or cloud.
- Disputes related to purging user data or applications must not default to licenses and arbitration processes that restrict the user's legal options.
- Users' consent for a device or web service to collect or infer data about them may not be interpreted to extend to information about their connections such as friends, contacts or affiliates.
- A legally mandated age of consent must protect minors by restricting the collection and use of private information.

- The need to protect personal information collected must not prevent access needed to allow 3rd parties of the users choosing from access to the data needed to maintain and repair devices.
- Remote access to devices must be protected from abuses that might create physical risks or loss of information.

Notification:

- Users must be informed promptly and directly, if their private information is lost, compromised, or misused. Organizations collecting, inferring or storing that information are responsible for the notification.
  Users must have the right to know the source of privacy violations and the responsible parties, whenever possible.
- Clear information must be available notifying recipients of paid advertising and content, along with a clear link to the source of that material and the intended beneficiary of the desired action.
  For online content, available metadata should lead to sponsoring site(s), allowing the user to utilize the transparency and disclosure rights indicated above.

This statement was developed by the IEEE-USA Committee on Communications Policy and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the over 150,000 engineering, computing and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.