

Digital Personal Privacy, Awareness and Control

*Adopted by the IEEE-USA
Board of Directors (22 June 2018)*

IEEE-USA supports greatly strengthening laws and regulations protecting individual digital privacy in this era of big data, analytics, and artificial intelligence. The United States 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 face recognition, voice recognition, and electronic identifiers (chips, devices), can be 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 can then be 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.

It is IEEE-USA's position that individuals need strong legal protection for their privacy. Fundamentally, U.S. law must recognize that individuals own information collected about them.

Examples of specific areas where increased protections are needed include:

Public Transparency:

- The public must be able to learn: the types of data being collected by any web site or other electronic means; what data is retained; how it is used; and what is shared with third parties, directly or indirectly. The same information must be available from those third parties.
- All data collection mechanisms must be disclosed to users, including web beacons or other mechanisms for tracking user activity or data. Disclosed information must be sufficient for users to identify and utilize their privacy rights.
- Each web site and application must disclose ongoing content placed on the user's device and the uses of that content.
- These disclosures must be accessible and comprehensible to the average user without specialized knowledge.

Disclosure for Users:

- For each web site and application, users must be able to obtain complete disclosure of the information that is retained by the site, application or third party accessing the user's information – directly or indirectly.

Control:

- Users must be able to remove personally identifiable data easily from any site, cloud or collection devices.
- Users must easily be able 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 web site to collect data about them may not be interpreted to extend to information about their "friends," or "contacts."
- A legally mandated age of consent must protect minors by restricting their release of private information.

Notification:

- Users must be informed promptly and directly, should their private information be lost or misused. Organizations collecting 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 consumer 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 more than 180,000 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.