LEAGUE OF WOMEN VOTERS® OF OREGON

**Position Statement: Privacy and Cybersecurity**
**Adopted: January 8, 2021**
**Amended: January 19, 2021**

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. This position statement addresses Elections, Information Security, Personal Information Protection, and Electronic Business and Social Media.

## Elections Security

The election process is the foundation of our representative form of government. Election integrity, accuracy, transparency and trustworthiness require vigilance to ensure security protections. Security requirements include and are not limited to:

- verifiable ballots;
- ballots that can be recounted and audited;
- up-to-date hardware and software, supported by venders, tested, and secure;
- protected voter registration databases;
- election staff/volunteers with cybersecurity expertise;
- cyber-damage contingency plans;
- risk-limiting audits;
- attention to disinformation and misleading ads.

Protect voters' ability to exercise an informed opinion on electoral matters. Explore limiting the unfettered electronic circulation and amplification of election misinformation (e.g., targeted disinformation campaigns, manipulated media, anonymous disinformation, and algorithmic and robotic disinformation campaigns).

## Information Security

Government, individuals, and organizations (including private sector and critical infrastructure), all require strong cybersecurity protections and effective deterrents to assure national security, economic and social stability, and personal information integrity.

- Create consistent information privacy laws and regulations across all organizations (government, private, for-profit, and non-profit) that eliminate gaps, inconsistencies, and overlaps.
- Regulate all technology-enabled organizations (e.g., internet platforms, online intermediaries, business-to-consumer platforms), not shifting sectors, so that organizations are subject to a uniform set of laws and regulations.
- Regulate all categories of information in the same way, regardless of the type of organization or sector that collects that information.
- Apply a baseline set of regulations to all types of information, regardless of type of organization or sector collecting that information.
- Apply regulatory requirements to organizations according to their size and complexity, the nature of data covered, and the risk posed from exposing private information.

- All information (including third-party data transfers) needs sufficiently flexible protections to address emerging technologies and scientific evidence while serving the common good by balancing the demands of stakeholders and vested interests.

The ubiquitous information and communication technologies (ICT) of today's pervasive digital services, platforms, and marketplaces require a global governance perspective to address their societal and economic impacts:

- Harmonize laws and regulations across jurisdictions to protect individuals and assure trustworthy flow of information across all boundaries—government, organizations, industry sectors, states, and countries.
- Aim to develop flexible regulatory structures that can quickly adapt to social and scientific realities and technical and economic policy challenges.
- Use forward-looking, collaborative mechanisms such as experimentation and learning, test-and-evolve, and post-hoc effectiveness reviews. Incentivize specific outcomes that facilitate anticipating and adapting to rapid changes.

State laws which become inconsistent with future comprehensive federal privacy standards may be preempted, while more stringent laws may remain. At a minimum, citizens' information protection rights should be comparable to those of citizens around the world—both current and future protections that may be established. Current European Council personal information protections include the ability to:

- be informed of what personal information is held and why
- access information held by an entity
- request updating or correcting of information
- request manual processing in lieu of automated or algorithmic processing
- request transfer of information to another entity
- withdraw prior consent to process data or object to specific situation consent
- request deleting personal information.

**Personal Information Protection**

Uniform privacy rights need to protect personal privacy and prevent known harms.

- Establish uniform information protections for personal and behavioral data that can be linked to an individual or devices.
- Prevent harmful uses of personal information by all information processors who collect, store, analyze, transfer, sell, etc.
- Expand the legal definition of "harm" to include physical, monetary, reputational, intangible, future, or other substantial injuries and to provide individuals the right to legal remedy.
- Assure that personal information collection, use, transfer and disclosure for economic or societal purposes is consistent with the purpose for which individuals provide their data, and does not cause them harm.
- Shift the focus of information protection from individual self-management when submitting data (e.g., opt-in, obscure notice, and choice disclosures) to organizational stewardship in protecting individuals' personal privacy.
- Expand personal information privacy definition to address rapidly changing information and communication technologies, accelerated networking between businesses, and automated collection and dissemination of data, which together subvert personally identifiable information, de-identification, re-identification, and data anonymization.

LEAGUE OF WOMEN VOTERS® OF OREGON

**Electronic Business and Social Media: Cybersecurity Responsibilities**

Organizations conducting electronic business and social media commercializing personal information both bear the responsibility for protecting information and must be liable for failure to protect individuals from harm.

All organizations--including third-party receivers:

- Must protect individuals' transferred information across multiple organizations to ensure end use accountability.
- Have a duty to safely collect, use, and share personal, sensitive information.
- Should use comprehensive information risk assessments, take proactive measures to implement information security measures, and be held accountable for fulfilling these risk management obligations.
- Are held accountable for misuse of personal information by strengthening both state and federal laws, rule-making, and enforcement powers.

We support the right of free speech for all. The digital tools of information and communication technology (such as algorithms and artificial intelligence) can selectively distort or amplify user generated content. The resulting disinformation, digital manipulation, false claims, and/or privacy violations may endanger society or harm others.

- Compel private internet communication platforms (applications, social media, websites, etc.) to be responsible for moderating content.
- Define liability for damages and provide for enforcement for failure to moderate content.