LEAGUE OF WOMEN VOTERS® OF OREGON

PARTICIPANT'S CONSENSUS WORKSHEET: *Privacy and Cybersecurity*

INSTRUCTIONS FOR COMPLETING CONSENSUS DISCUSSION WORKSHEET
Read the Privacy and Cybersecurity study
Review the following two-page summary of study policy findings (pp. 1-2)
Complete your pre-discussion worksheet (pp. 3-7)

Summary of Study Policy Findings [Refers to Consensus Propositions]

In the digital age, it is increasingly challenging to protect the personal identity and privacy of individuals, and to provide the open, secure flow of information in cyberspace for the benefit of individuals and society. Efforts to address privacy and cybersecurity policy concerns today are complicated by the increase in big data, E-commerce, and artificial intelligence. A 2014 Pew Research Center study found that 91% of consumer think they have "lost control over how their personal information is collected and used by companies." (Madden, 2014).

The US Constitution does not recognize an explicit right to privacy, nor does the US have a single, comprehensive Federal privacy law. Current policy debates focus on *personal information privacy* to protect an individual's identity, while *cybersecurity* policies protect information access. Personal data protections are based upon a mix of differing Federal and state statutes and rules, common law precedents and business practices. This patchwork of laws and regulations creates a fragmented set of statutes with different privacy protections for individuals and different compliance requirements for public and private sector institutions.

US PRIVACY POLICY IS NOT UNIFORM [Refers to Worksheet Part II Propositions]

These factors contribute to policy fragmentation:

- Federal laws primarily apply to how the Federal government handles personal information in order to protect individuals from intrusive government.
- Federal laws applying to private sector organizations narrowly target specific sectors and certain types of sensitive personal information, including health, credit, financial, telecommunications, and children's and student information.
- Sector-level regulation typically takes the form of industry self-regulation and enforcement of voluntary on-line privacy protections. Firms that gather, analyze, and distribute consumer information self-regulate and voluntarily define how they will handle responsibility for individual's information, including sharing with third parties. Recent consumer protections enacted or pending in several states are expected to overhaul current practices.
- Sector-level data regulation means many businesses are not regulated; sector-level regulation does not adequately address the practices of firms that cross sectors to use data technologies to compete in other businesses (e.g., media, retail, etc.).
- In the absence of comprehensive Federal privacy protections, states have begun to enact their own privacy requirements for the private sector, creating inconsistent and/or conflicting laws from state to state.
- Regulation tends to target specific violations and past abuses (e.g., breach notifications, employer access, data tracking, data brokers, etc.). Emerging problems which are difficult to anticipate are often beyond the reach of existing regulations, and regulatory mechanisms can be designed to address future concerns.

LEAGUE OF WOMEN VOTERS® OF OREGON

INDIVIDUAL AND PERSONAL DATA PROTECTION [Refers to Worksheet Part III Propositions]

There are several ways in which changing technologies are prompting a rethinking of personal data protection. Some experts recommend adopting *use-based policies* to prevent harmful *use* of sensitive data. Use-based policies focus on data end use rather than controlling data access or transmissions, and apply to the original data and any subsequently derived data. Both current understandings of personal information and redress for data violations continue to evolve.

Current laws focus on personal data privacy, particularly *Personally Identifying Information* (PII), which is unique to an individual (e.g., account numbers, social security numbers). The surge in big data means a wide array of non-unique information can be used to reidentify supposedly anonymous individual data. Regulating an individual's PII is fast becoming obsolete. Some experts recommend that privacy protection be applied to all *identified and identifiable* persons.

E-COMMERCE DATA PROTECTIONS [Refers to Worksheet Part IV Propositions]

E-Commerce is a business model driven by consumer data where private sector firms use data tracking and big data analytics to profit from personalized advertising. In the US, the Federal Trade Commission (FTC) oversees consumer information privacy, enforces data protection regulations, and protects consumers against unfair or deceptive business practices. Using voluntary self-regulation, firms that gather, analyze, and distribute consumer information define how they will handle responsibility for individual's information. The FTC encourages on-line businesses to adopt fair, transparent privacy practices, and may act to assure firms comply with their own stated practices.

- E-commerce treats individual data as a commodity, turning consumer profiles found in big data into a highly profitable industry that packages and sells personal data to third party users which are often unregulated.
- Sector-specific privacy regulation is complex and variable;
  - It is not clear how firms protect specific personal information.
  - It may not cover information transferred to a third party, and data protections are lost as data changes hands.
  - It creates inconsistent coverage; some businesses are subject to multiple overlapping requirements and others have few requirements.
  - It does not address businesses that operate in multiple sectors or that expand into new business sectors, creating gaps in privacy protection.
- Self-regulation has weaker enforcement mechanisms than direct regulation and consumers have limited recourse for violations.
- The FTC relies on consent agreements to remedy business fair practice violations because it does not have authority to impose fines.

End of Policy Findings Summary

LEAGUE OF WOMEN VOTERS® OF OREGON

PARTICIPANT'S CONSENSUS WORKSHEET: Privacy And Cybersecurity

PRIVACY AND CYBERSECURITY CONSENSUS PROPOSITIONS FOR DISCUSSION

These propositions are broad, overarching statements about key elements of a comprehensive policy framework, individual privacy protections, requirements for E-Commerce, and election cybersecurity.

We are seeking your League's view on which of these options are most valued.

These propositions are designed to determine what dimensions of privacy protection should be strengthened under Federal and/or state law. The current US privacy framework is an uneven mosaic of laws and regulations that makes individual consumers responsible for much of their own privacy protection and gives business sectors varied levels of responsibility and freedom in how they protect personal data. Experts have recommended adopting the options below, including how to implement them, but policymakers have not acted on their recommendations.

The following policy choices have been considered by a wide range of experts, including lawmakers, tech industry and security experts, legal and privacy experts, academics, and think tanks. These consensus propositions are framed as national policy choices which must ultimately be addressed because the internet transcends state and national policy. Important issues identified through consensus will serve as the basis of LWVOR's state-level position, and also submitted to LWVUS national conference for consideration.

INSTRUCTIONS: After reading the Privacy and Cybersecurity study, please complete this worksheet to indicate your initial views. *Based on your current knowledge, use the scales below to assign 'importance' ratings to each lettered proposition.* Bring this completed worksheet with you to use in consensus discussions. Thanks for your valued input.

PART I: ELECTION SECURITY

Based on your current knowledge, use the scales below to assign importance ratings to each lettered proposition.

a. Replace paperless voting machines with systems that create a voter-verified paper backup of every vote.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Replace outdated hardware and software that can no longer be serviced.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Upgrade registration databases for better security.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

d. Increase cybersecurity expertise for election office staff and volunteers.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

e. Develop contingency plans to mitigate potential cyber damage.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

f. Check and confirm electronic tallies with post-election audits comparing paper ballots and voting machine totals.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

g. Regulate election-related disinformation and misleading political ads

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments

PART II: PRIVACY POLICY SHOULD BE UNIFORM AND CONSISTENT

Use the scales below to rate the importance of each of the lettered propositions.

1. The scope of the United States' legal privacy framework should…

a. Define different privacy protections for specific types of data.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Tailor specific privacy protections to different types of businesses (tech firms, banking, healthcare, etc.).

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Define uniform privacy protections for all personal data.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments

2. The United States' legal privacy framework should…

a. Assure data transferred to other entities continues to have the same, enforceable privacy protections.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Adopt flexible practices capable of addressing emerging concerns like big data, artificial intelligence, smart technologies and future innovations.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Reconcile gaps, inconsistencies and exceptions in privacy laws and regulations across federal, state, and regulatory agencies.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments

PART III: INDIVIDUAL AND PERSONAL DATA PROTECTION

Use the scales below to rate the importance of each of the lettered propositions.

a. Define uniform privacy rights for all consumers.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Apply privacy protection to all identified and identifiable (with big data analytics) persons.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Focus laws and regulations on preventing known harmful uses of sensitive personal data.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

d. Redefine legal definitions of data violation 'harms' to include certain intangible harms and future risks such as identity theft and fraud.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

e. Provide for judicial remedy by granting consumers the right to sue companies that violate their personal information protections.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments

PART IV: E-COMMERCE DATA PROTECTIONS

Use the scales below to rate the importance of each of the propositions.

a. Require all businesses that process or control personal data to establish effective governance and accountability programs.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Require all businesses that process or control personal data to be responsible and accountable for any and all subsequent end uses of personal data, including transferred data.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Make third party data processors and data holders responsible stewards of personal information, protecting individual users' interests and accepting liability for harms to individual users.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

d. Require meaningful consent protocols that assure consumers are clearly informed with specific and unambiguous information (including specified purpose and use of data), and that consent is freely given, without coercion.

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

e. Strengthen Federal Trade Commission authority to require data accountability programs and impose substantive penalties for privacy violations

Importance of this element to policy:

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments

PART V (Optional): EUROPEAN UNION INDIVIDUAL PRIVACY RIGHTS

Your League is not required to complete consensus on this optional section. However, completing consensus on it will provide further information for developing a final League position.

The following set of individual privacy rights are current standards in use in the European Union. Some US companies may be required to comply with these standards.

Rating these statements will provide further information for developing a position; however, your League does not need to discuss to reach consensus on them.
Rate the policy importance of these individual rights that currently apply in the European Union.

a. Right to be informed about the personal data organizations have about them

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

b. Right to access personal data

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

c. Right to rectification – correct errors in personal data or add to incomplete records

☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

d. Right to erasure* (aka, “the right to be forgotten”)
[*i.e. create a process for individuals to request that Internet search engines remove certain results]
☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

e. Right to restriction on processing of personal data
☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

f. Right to data portability
☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

g. Right to object to the processing of personal data
☐ Essential ☐ Important ☐ Low Importance ☐ No Opinion

Comments