February 8, 2023 PPOC meeting

WHITNEY PHILLIPS & NORA KURZOVA
State Privacy Office (SPO)

OFFICE OF THE
STATE
AUDITOR

Mission

Provide a safe experience to constituents, especially youth, while safeguarding their privacy and mitigating risks.

S.B. 152/ H.B.311 - Social media amendments

- **ISSUE 1** - Un-redacted ID forms of **all users of** Social Media Companies (SMC) required to be provided to the SMC or to an unspecified 3rd party. (privacy risk)
- **ISSUE 2** - Forbids access to SMC services to persons under 18 and at night without a verified parental consent. (safety / privacy risk)
- **ISSUE 3** - Mandates automatic access to minors' accounts in its entirety to parents/guardians. (privacy risk)
- **ISSUE 4** - Establishes a rebuttable presumption of harm for users under 16 years. (weakening of a key legal doctrine)

Comparison: Utah resident may seek to be employed at 14 years of age, may drive a vehicle at age of 15, and obtain a handgun at age of 18.

S.B. 152/ H.B. 311 - Recommendations

- **ISSUE 1** - Reconsider age-gating the interactive internet as the action impacts estimated 90% / 3 million Utah residents.
- **ISSUE 2** - Require that SMCs offer users various methods of age verification, such that do not require identity revealed/ full ID form provided. Examples include:
  - "Social vouch" by selected verified adults
  - "AI driven analysis" of user submitted video, where sensitive data is removed.
  - "Social code" store-bought vouchers, age verified during the purchase.
- **ISSUE 3** - Reconsider limiting access by default to "parents of children below 13" to align with COPPA, or remove "entirety." Examples of more adequate oversight include automatic parental access to metadata only. (whom/to/subjects/public/frequency)
- **ISSUE 4** - reconsider automatic presumption of harm having occurred

WHEN, WHO, WHO HAS ACCESS TO DATA

- BEFORE 2020 - **“Private voter”** □ Gov. Officials only

- 2020 - 2023 - **“Private voter”** □ Gov. Officials, Pol. Part, Candidates, Vol., Cont.,
  “Withheld voter” □ Gov. Official only (all data)

- AFTER 2023 - **“Protected Individual”** □ Identifying data goes to Gov. Officials
  □ Non-Identifying: Gov. Ofs, Pol.P., Cand., Vols.

- **What belongs to Non Identifying data?**
- Pseudonym of name+address, residential address, voter history, precinct, affiliation, age group

- **Data shared by default**: name, address, political affiliation (non-exhaustive list)

- **Never shared** outside of government: Driver’s license number, SSN, Full birthday, Email, Phone

H.B. 303 – Election records amendments

- **ISSUE 1** – improper collection of sensitive data – required to label individuals "victim of domestic violence" or "likely victim" to get status of "Protected individual." (privacy risk)
- **ISSUE 2** – lack of legal certainty – introduces terms "identifying" information, and "small number" without providing / referring to a specific definition. (undesirable legal practice)
- **ISSUE 3** – misleading and creates disparity. Those who registered as private voters before 2020 will lose some protections, while becoming "protected individuals". New voters will not get the opportunity for the same privacy protections. (privacy/legality risk)
- **ISSUE 4** – using pseudonymization techniques relying on its irreversibility and presuming complete absence of re-identification. (security/privacy risk)

H.B. 303 – Recommendations

- **ISSUE 1** – do not require collection of sensitive data as a prerequisite to enjoy further privacy protections.
- **ISSUE 2** – introduce definition, exact scope or reference to a legally established terms, minimize scope of data as well as groups with access to "withheld voter" / "protected individual."
- **ISSUE 3** – allow "withheld" category for all voters and limit its scope to match "private" from before 2020.
- **ISSUE 4** – rely on anonymization instead of pseudonymization standards.

S.B. 127 - Cybersecurity Amendments

Utah Cyber Center

a) develops and maintains a statewide strategic cybersecurity plan for executive breach agencies and other governmental entities;

b) Supports executive branch agencies;

c) When requested, supports other governmental entities;

d) Promotes cybersecurity best practices;

e) Share cyber threat intelligence with government entities;

f) Serve as the state cybersecurity an incident response hotline to receive reports of breaches of system security;

g) Develop incident response plans to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology system within the state; and

h) Coordinate, develop, and share best practices.

S.B. 127 - Recommendations

Include state privacy officials in Utah’s Cyber Center

H.B. 168 – License Plate Reader Systems Amendments

- **ISSUE 1** - warrant requirement removal (privacy risk)
- **ISSUE 2** - lack of quality control - no review of privacy policy by experts, inappropriate logging (privacy and security risk)
- **ISSUE 3** - lack of transparency – absence of notice on locations of stationary devices and purpose of data collection (privacy and public trust risk)

H.B. 168 – Recommendations

- **ISSUE 1 -** keep probable cause and warrant requirement.
- **ISSUE 2 -** include a mandatory review of privacy policies by SPO and establish more detailed logging requirements.
- **ISSUE 3 -** include a requirement to place easy to see and understand notice where stationary devices reading plates are placed.

H.B. 158 – Electronic Information or Data Privacy Act Modifications

- **ISSUE 1 -** warrant requirement removal (privacy risk)
- **ISSUE 2 -** amendments include overly broad language.

Examples include:

- "appears to pertain to dishonesty" as a reason for disclosing personal information by a provider of telecommunication services.

- "audio-video surveillance recording" without further clarification regarding the scope, format and method of recording. (privacy and public trust risk)

H.B. 158 – **Recommendations**

- **ISSUE 1 -** keep probable cause and warrant requirement.

- **ISSUE 2 -** remove "dishonesty" as a qualifier, describe scope, format and method of collecting data that would qualify as "audio or video surveillance."