

UTAH PRIVACY COMMISSION
FY 2026 Report to the Judiciary Interim Committee
September 30, 2025

The Utah Privacy Commission issues this report pursuant to Utah Code §63A-19-202(3). The Utah Privacy Commission's FY 2025 Data Privacy Agenda and Report to the Utah Privacy Governing Board is attached to this report. The Commission has five working subcommittees:

- Government Privacy Standards and Best Practices;
- Government Privacy Education and Training;
- Government Privacy and Civil Liberties;
- Government Privacy and Cybersecurity Legislation; and
- Government Privacy Impart Assessments.

The subcommittees preview issues for, and make recommendations to, the Commission, which then votes on the same. The Commission typically meets monthly at the Capitol complex. In order to better acquaint the public and government stakeholders about the Commission's work, some meetings are conducted in other locations. Our February 12, 2025 meeting was held at the Heber Wells Building, and our September 10, 2025 meeting was held at the Davis Conference Center as part of the Utah Association of Counties annual conference. That meeting created an opportunity for a dialogue with county officials concerning their experiences in implementing the Government Data Privacy Act. In addition, several Commissioners actively participated in the Government Data Governance Summit held at Utah Valley University on May 29, 2025.

The Results of Reviews the Commission has Conducted

Educational and Training Materials: The focus this year for the Commission was to continue to monitor and discuss educational and training materials as they are developed by the Office of Data Privacy, the State Privacy Auditor, and others. Based upon monthly reports from the Government Privacy Education and Training Subcommittee, the Commission was able to:

1. Hold a number of training and management sessions to take reports from local government officials on the impacts of the privacy framework and the value that the offered training has had at the local level;
2. Work with the Utah League of Cities and Towns and Utah Association of Counties and other local government organizations to set up a yearly training course at those organizations' conferences; and
3. Work with the Office of Data Privacy to ensure that the online training resources that are being developed are compatible with various platforms.

Privacy Impact Assessments: The Government Privacy Impact Assessments subcommittee actively monitors the development and use of Privacy Impact Assessments, including the administrative burden that completing PIAs places on government entities.

Reports by the Office of Data Privacy, the State Privacy Auditor, and the State Privacy Ombuds: The Commission typically receives a monthly report of recent achievements by the Office of Data Privacy and the State Privacy Auditor. These reports include new initiatives, results of surveys, and other useful information. The State Privacy Ombuds also gives periodic reports several times a year.

Other Reviews: The Commission reviews other practices as well. Some recent reviews include the use of automatic license plate readers, the use of “phone home” verification systems, and state endorsed digital identities.

The Guiding Standards and Best Practices

The Government Privacy Standards and Best Practices subcommittee is working closely with the Office of Data Privacy to review best practice recommendations, which it then reports to the full Commission. In particular, the Subcommittee is working with the Office of Data Privacy to provide best practice recommendations for privacy related contract terms and conditions as advice to local governments on third-party vendor agreements. These best practice recommendation will soon be posted at the Office of Data Privacy's website, privacy.utah.gov. The Subcommittee is also working on more general standards and best practices, but does not have final results in those areas yet. The Subcommittee was also the genesis for some of the legislative recommendations discussed in the next session.

Recommendations for Legislation

The Government Privacy and Cybersecurity Legislation subcommittee evaluates possible legislation concerning data privacy and government and makes recommendations to the full Commission which are discussed and voted on in open meetings. This year, the Commission recommends that the Legislature consider the following possible legislation:

1. The Legislature should consider passing a version of the 2025 General Session Bill HB 468, Automatic License Plate Reader Amendments. The final bill should be a consensus of major stakeholders, including law enforcement.
2. When the Legislature considers regulating the use of AI in government hiring and employment decisions, it should consider a bill that provides a:
 - **Transparency and Notice Requirement** (provide applicants and employees with an explanation of the AI process and its use for evaluating applicants and employees;

employers would be required to notify applicants and employees, in writing, when AI tools are being used in decision-making processes)

- **Consent Requirement** (obtain the applicant’s consent for such AI use)
 - **Impact Assessment Requirement** (require impact assessments for AI hiring tools to better understand their potential negative effects and to identify strategies to mitigate those effects)
 - **Human Oversight Requirement** (any employment decision influenced by AI would be required to pass through meaningful human review)
 - **Data Privacy Requirement** (ensure that data used in AI-decision making strictly adheres to data protection regulations)
 - **Robust Auditing Requirement** (conducting regular audits of AI tools and bias testing will be essential to mitigate risk of algorithmic bias and discrimination)
3. Before implementing any artificial intelligence tool that may impact privacy of individuals or their civil liberties, or contribute to decision-making, a law enforcement agency shall:
 - Conduct a Privacy Impact Assessment (PIA) in order to identify and evaluate potential risks to privacy and civil liberties;
 - Document the measures implemented to mitigate risks identified in the PIA; and
 - Ensure the PIA is publicly available unless disclosure would compromise law enforcement operations or public safety."
 4. The legislature should ensure that progress is ongoing with respect to the State Endorsed Digital Identity (2025 Session SB 260), which was a landmark bill that gained worldwide notoriety by how it specifies and supports the unique identity and privacy rights of the individual, as well as, how “the state is obligated to respect and individual’s privacy interest associated with the individual’s identity.” We encourage the Legislature to now authorize the several processes for establishing a state-endorsed digital identity (SEDI) program. Such processes include (but are not limited to): requirements gathering and refinement, solicitation of candidate technologies, security and privacy analysis of submitted candidate technology proposals, etc. These processes will help Utah to evaluate multiple technology approaches for their respective security and privacy capabilities in order to establish the SEDI infrastructure.
 5. The Legislature should consider augmenting the privacy legislation currently protecting Utahans by introducing a legislation that specifically precludes “phone home” verification processes from use in government systems. In critical digital credential processes, (e.g., verifying and validating digital credentials), some systems have created a means for a credential verifier (e.g., school, store, etc.) to connect to a credential issuer (e.g., state

government) to determine if a credential is still valid. This simple process creates significant privacy concerns by allowing issuers (and potentially other parties) to track when and where a person is using their credentials. Furthermore, “phone home” verification can put Utah’s digital credential verifiers (e.g., stores, banks, resorts, etc.) in a position of reporting back to foreign government issuers, which could assist their state surveillance of their citizens. This also presents a potential cyber security vulnerability by enabling foreign governments to record the computer’s IP address, which could be used in future Denial of Service (DoS) attacks. Current technology exists that allows digital credential verification without contacting an issuer. It will further enhance and protect Utahans privacy to prohibit “phone home” based verification systems in current and emerging Utah government identity systems.

6. The legislature should consider streamlining the Utah Privacy Commission’s reporting requirements under the GDPA, [Utah Code Section 63A-19-204](#)(1)(3), (3), and (4). Too much of the Commission’s time is spent on three very similar annual reports. At the same time, the ridged reporting cycle limits the ability of the Governing Board to effectively oversee the UPC as new issues arise in the rapidly changing world of data privacy. The UPC recommends keeping the annual report to the Judiciary Interim Committee in Section 204(3), eliminating the other two reports, and adding provisions that provide: (a) for the Governing Board to require that a Commissioner give an oral update on the work of the Commission at any Governing Board meeting if requested, and (b) providing that the Governing Board may at any time instruct the Commission to investigate, report upon, or not investigate any issue of governmental privacy within the scope of the Commission’s duties.
7. The legislature should consider adding a provision that say that the Commission “may endorse” any policy, practice, or report of the Office of Data Privacy or the State Privacy Auditor. This would give formal recognition to the role of the Commission in reviewing such actions, and would legitimize such polices by giving them a public hearing, while not giving the Commission an actual veto over any work by the ODP or the UPA.
8. The Legislature should consider amending [Utah Code Section 63A-19-101](#)(33) to broaden the definition of “sell” to include exchanges for value that are not necessarily monetary, such as allowing a vendor to use personal data for its own marketing purposes that it acquires in the course of performing a contract for a governmental entity.
9. The Legislature should consider amending the GDPA and GRAMA to prevent private corporations from exploiting public records for commercial gain without providing a direct benefit to the state or its citizens. This may be achieved through measures such as implementing or increasing data or records user fees, particularly on mass transfers of data, to generate state revenue, while also protecting individual privacy and preserving governmental transparency. Large-scale commercial applications of public records include the transfer of ownership, the sale of personal data, data reidentification, and the use of records to train artificial intelligence models.

Adopted by vote of the Utah Privacy Commission on September 30, 2025.