

Technology Transparency Stu

...

UPC & ODP

Current Requirements (GDPA)

“A governmental entity shall provide a privacy notice to an individual, or the legal guardian of an individual, from whom the governmental entity requests or collects personal data.”§63A-19-402 (1)

“The office and the commission shall jointly study the implementation of processing activities for which an individual's personal data may be collected without ~~the ability to~~ **provide direct notice**” §63A-19-407(1)

Transparency Study Topics:

When personal data is collected without the ability to provide direct notice, the study shall address:

- (a) the public safety benefits and legitimate governmental purposes served;
- (b) the privacy implications of the processing activities; and
- (c) appropriate frameworks for governing the processing activities.

See §63A-19407(1)

Potential Examples of Notice-Exempt Processing

Processing Activity	Source Type	Direct Notice Possible	Core Purpose
911 calls/emergency response recordings	First-Person	No - emergency setting	Emergency response - dispatch coordination; real-time incident assessment
License plate readers (LPR)	Second-Person	No - scale is impractical	Surveillance & tracking - vehicle identification and evidence provision
Cell site simulator (CSS)	Second-Person	No - scale is impractical	Criminal investigation - locate and track device location
Drone monitoring (targeted)	Second-Person	No - self-defeating	Criminal investigation - suspect surveillance; evidence gathering
Drone monitoring (general)	Second-Person	No - scale is impractical	Public safety monitoring - crowd monitoring and creating records
Undercover officer interactions (in-person or	Second-Person	No - self-defeating	Criminal investigation - infiltrate networks; gather evidence covertly
Dash/body cam incidental capture	Second-Person	No - scale is impractical	Evidence collection - document encounters
Transit system surveillance	Second-Person	No - scale is impractical	Public safety monitoring - deter crime; monitor incidents
School mandatory reporting systems	Third-Person	No - self-defeating	Public safety monitoring - monitor individual safety
Accessing utility usage records	Third-Person	No - scale is impractical	Evidence collection - detect anomalies; support investigations
Accessing health data	Third-Person	No - scale is impractical	Regulatory enforcement & compliance - verify claims; investigate misuse
Accessing credit reports	Third-Person	No - scale is impractical	Identity, verification & risk assessment - assess financial status/eligibility
Accessing cell site location information	Third-Person	No - scale is impractical	Criminal investigation - reconstruct movements; place suspects
Accessing marketing lists	Third-Person	No - scale is impractical	Identity, verification & risk assessment - locate individuals; enrich profiles
Data matching / fraud detection systems	Third-Person	Plausible	Benefits administration - detect fraud; verify eligibility

Some Options for Project Steps

1. Identify and prioritize the processing activities at issue
2. Agree on precise terminology/classification
 - a. Test/revise using a pilot survey
3. Draft data collection tool (survey)
 - a. Stakeholder respondents will be given processing activities
 - b. They will then be asked to rank/rate the importance of relevant safety benefits/ privacy concerns + plausibility of providing notice for each processing activity
4. Administer survey to stakeholders (law enforcement, civil liberties groups, etc.)
5. Conduct hearings to investigate survey patterns and gain additional information
6. Synthesize results
7. Develop legislation recommendations for consideration by the full UPC

Example response: School reporting

Processing Activity	Source Type	Direct Notice Possible	Core Purpose
School mandatory reporting systems	Third-Person	No - self-defeating	Public safety monitoring - monitor individual safety

- **Public safety benefits:**
 - Identification of at-risk individuals → High priority
 - Enables timely intervention by authorities → High priority
- **Privacy concerns:**
 - Risk of false reporting → High priority
 - Limited ability to challenge or correct information early → Medium-High priority
- **Notice: selfdefeating, legally restricted in many cases**
 - Post hoc notice may be plausible in some cases*

Goals and Deliverables

- Standardized classification of notice-constrained processing activities, what qualifies as direct notice, etc
- Identify where restrictions are needed/politically viable and where consensus supports alternatives (e.g., audits, post hoc notice)
- Data from interviews, surveys, and hearings that will support conclusions
- Legislative recommendations

Suggested Early Priorities

- Set up a UPC task force of up to five commissioners
- Coordinate between the task force and the Office of Data Privacy
- Agree on precise terminology/classification
- Determine if the report can be done by November of 2026 instead of 2027
- If not, determine if a partial report focused on specific areas is possible by November of 2026
- Set timelines for:
 - Surveys;
 - Hearings including key stakeholders; and
 - A draft report or partial report.
- Report back to the full UPC regarding the above by their 8th meeting