

General Government

Updating the Colorado Privacy Act for the Age of Artificial Intelligence	
Gunnison County (Commissioner Liz Smith)	
Preferred Contact:	Liz Smith, Gunnison County eksmith@gunnisoncounty.com; 303-350-3954
Co-Sponsoring Counties/Commissioners:	N/A
Who is your subject matter expert?	Jefferey Riester Director of Legislative Affairs / Senior Assistant Attorney General Jefferey.Riester@coag.gov
Has this proposal been approved by your BoCC?	No.
Have you reviewed the CCI Instructional Memo?	Yes.
Describe the problem your proposal will solve.	The enactment of the Colorado Privacy Act (CPA) in 2021 established important consumer rights and created a framework for the responsible collection, use, and protection of personal information. The law provides Colorado residents with rights to access, correct, delete, opt-out, and limit the use of their personal data and creates obligations on businesses that collect and process that information. The CPA and its implementing regulations also recognize that sensitive inferences derived from personal data warrant protection. Since the CPA's enactment, however, advances in artificial intelligence, machine learning, and large-scale data integration have fundamentally changed how businesses create, control, and commercialize information. Rather than simply collecting personal data, many AI-enabled systems generate proprietary datasets—including persistent object identifiers, behavioral signatures, movement histories, confidence scores, and predictive models—from combinations of customer data, publicly available information, and automated analysis. These datasets are often commercially valuable in their own right and can be used to identify, re-identify, or track individuals across time, systems, and jurisdictions. The CPA provides limited guidance on when the aggregation of otherwise public information becomes regulated personal data, how AI-generated proprietary datasets should be classified, or when entities that create and control these datasets assume the responsibilities of data controllers.

	Examples: •Automated License Plate Reader (ALPR) systems. Modern ALPR platforms operate as multi-jurisdictional surveillance networks that generate proprietary datasets from thousands of cameras. While local agencies may access only a limited subscription, vendors can create and retain searchable movement histories, object fingerprints, behavioral patterns, and other AI-derived datasets that are not publicly available and may be shared across subscription networks, including with out-of-state or federal entities. •AI-enabled behavioral health services. AI counseling platforms increasingly collect highly sensitive information about mental health, trauma, substance use, and emotional well-being. Although the CPA regulates sensitive data, important questions remain regarding AI-generated behavioral profiles, inferences, model outputs, and other proprietary datasets created outside traditional healthcare privacy frameworks such as HIPAA. This issue is particularly relevant to counties because local governments increasingly rely on private technology vendors to provide critical public services while having little ability to negotiate or oversee how vendors generate, retain, license, or share proprietary datasets beyond the services purchased by the county. Updating the CPA would establish clearer statewide standards governing AI-generated datasets and surveillance infrastructure, placing responsibility on the entities that create, control, and profit from those systems rather than expecting individual local governments to address these issues through contract negotiations alone.
Areas of Impact:	Power/Authority/Mandate of county government, General community advancement, civil liberties, consumer protections, health and human services
What is the ultimate source of this problem?	The CPA appropriately regulates many forms of personal data and sensitive data inferences, but it was enacted before recent advances in artificial intelligence, machine learning, and large-scale surveillance infrastructure fundamentally changed how information is created and used. Modern AI systems do not merely infer characteristics from personal data—they generate proprietary datasets, persistent identifiers, behavioral profiles, movement histories, and predictive models from combinations of personal data, publicly available information, and automated analysis. The CPA provides limited guidance on when these AI-generated datasets become regulated personal data, how they should be classified, or when the entities creating, controlling, retaining, licensing, and commercializing them assume the responsibilities of data controllers. As a result, businesses may develop and profit from commercially valuable

	surveillance datasets whose governance, retention, downstream sharing, and accountability are not clearly addressed within the CPA's existing framework.
What is your initial proposal to solve this problem?	The proposal would modernize the Colorado Privacy Act to address how artificial intelligence, machine learning, and advanced data analytics create, aggregate, and commercialize new categories of information. The legislation would clarify when AI-generated datasets, persistent identifiers, and other proprietary data products derived from combinations of personal data, publicly available information, and automated analysis become regulated personal data; strengthen standards governing de-identified and anonymized data in light of modern re-identification capabilities; extend protections for legally protected healthcare data; and clarify the responsibilities of entities that create, control, retain, license, or commercialize AI-generated datasets to ensure they are subject to appropriate privacy, security, retention, and accountability requirements.
Please provide sample language for this solution.	•Clarify "Personal Data." Amend the definition of "personal data" to specify that information generated through automated analysis—including AI-generated identifiers, behavioral profiles, movement histories, confidence scores, or other persistent identifiers—is personal data when it is linked or reasonably linkable to an identified or identifiable individual, regardless of whether it was derived from personal data, publicly available information, or a combination of data sources. •Define "Derivative Digital Identifier." "Derivative digital identifier" means an identifier or persistent representation generated through the automated analysis of personal data, publicly available information, visual, auditory, geospatial, or sensor data that is used or reasonably likely to be used to identify, re-identify, recognize, correlate, or track an individual, object, or device across time, systems, or locations, including identifiers derived from physical attributes, movement patterns, behavioral characteristics, or statistical confidence models. •Revise "De-identified Data" and "Anonymized Data." Clarify that data is not considered de-identified or anonymized if, considering all means reasonably likely to be used—including artificial intelligence, machine learning, aggregation, or other automated analysis—it can reasonably be used to identify, re-identify, recognize, correlate, or track an individual or to generate a derivative digital identifier or other persistent identifier. •Clarify Controller Responsibilities. Specify that an entity that creates, determines the purpose of, retains, licenses, commercializes, or otherwise controls AI-generated datasets, derivative digital identifiers, behavioral profiles, or other proprietary data products assumes the responsibilities of a controller with respect to those datasets, regardless of whether the original source data was provided by another controller or consisted of publicly available information.

	•Define "Legally Protected Healthcare Data." Expand sensitive data protections to include information that identifies, tracks, or reveals that an individual has sought, received, provided, or inquired about healthcare services lawful in Colorado, including through AI-generated profiles, location history, behavioral analysis, or associations with healthcare providers or facilities. •Amend Data Minimization (§ 6-1-1308). Clarify that AI-generated datasets, derivative digital identifiers, behavioral profiles, and other proprietary data products remain subject to the Act's requirements for purpose limitation, data minimization, retention, deletion, and consumer rights. The creation of such datasets shall not create a separate category of information exempt from the requirements of this part, and they may not be retained, licensed, transferred, or used for secondary purposes beyond those expressly disclosed and authorized under the Act.
Are there any solutions that do not require state-level legislation? Has your county explored these alternatives?	Counties cannot control vendor architecture, derived-data creation, downstream sharing, or retention practices through local action alone.
Has CCI or any other organizations sought a solution to this problem before?	The 2026 legislative session saw bills that proposed to regulate industries like ALPR companies by shifting compliance responsibility to the local level, and without addressing how to ensure compliance with out-of-state and federal governments (SB26-070, SB26-071). Another bill proposed to ban governmental purchase of personal data from third parties without addressing how companies are selling derived personal data that is not captured in statutory definitions (HB26-1037). That legislation similarly put the burden on local governments to navigate. Updating the CPA provides a structural solution that does not burden local governments. This may also reduce the opposition the above bills drew from entities like law enforcement agencies, human resources directors, etc.
What possible organization(s) would support your proposed solution?	Personal privacy is important to Coloradans across the political spectrum. Specific organizations that would likely support include: local government organizations; child welfare advocates; domestic violence organizations; immigration rights organizations; privacy organizations like Electronic Privacy Information Center; school privacy advocates; behavioral health, reproductive health, and healthcare organizations.
What possible organization(s) would oppose your proposed solution?	Tech companies and data brokers, AI platform and ALPR/surveillance providers

Have you spoken with any legislators about your proposed solution? If so, what was their response?	Yes. At least one is interested in sponsoring and views this as a more elegant solution than some of the legislation in 2026 focusing on specific technologies or commerce of data. AG's office is interested in CPA update as well.
What are the financial implications of this problem to your county? Are there any financial implications to this solution either?	The proposal would reduce liability exposure lawsuits that could be brought against local governments who increasingly rely on contracts for technology we can't fully control (e.g., violations of CPA, SB25-276, child privacy, etc.)
What are the financial implications of this problem to any other impacted parties? What are the financial implications of this solution to any other impacted parties? <i>Please consider any relevant Colorado State Departments.</i>	Businesses and vendors who create and process the types of data described in new definitions would incur costs to ensure compliance.
Staff Feedback	<u>Risk / Difficulty:</u> <u>Time Commitment:</u>