Will Carney's majority government usher in a costly era of privacy invasion?

Privacy protection continues to rate high in public polling. Yet recent legislative moves are violating that trust, and throwing personal data protection out the window.

By Ken Rubin, May 6, 2026

The Carney government prefers to focus on domestic major economic projects and overseas economic diversification rather than being overly concerned with the impacts and costs of its current and planned legislation that overwhelm Canadians' individual privacy.

There is various legislation underway that gravely weakens privacy protection that, with a weakened opposition and a soon-to-be lapdog House Privacy Committee, will face fewer roadblocks.

This includes Bill C-22, which would give police and intelligence agencies new surveillance powers to track and access internet, cloud, and telecom users' personal data accounts without a warrant.

The bill requires electronic service providers to build interception and surveillance capabilities directly into their networks, and to record and hold on to meta information on every person in Canada and abroad, including physical location and interaction data for up to a year.

That makes those systems vulnerable to outside hackers, hostile states, and cyber criminals.

Then there is Bill C-25, which would allow federal and provincial political parties to self-police, and to manipulate their personal data collection and uses rather than be subject to a regulatory system involving privacy commissioners.

The recently passed C-12 allows for greater sharing of sensitive personal information of immigrant and refugee applicants.

Two bills that may appear by 2027 are advertised as "modernizing efforts": one for remaking the public-sector 1982 Privacy Act, and one for redoing the 2000 private-sector Personal Information Protection and Electronic Documents Act (PIPEDA).

The Privacy Act changes, now under consultation, would permit personal data sharing, reuse, and integration for delivery of services that diminishes the need for individual consent and significant restrictions.

Canadians will get little to no information on all the uses of their personal data, while the government will be relying more heavily on unregulated technologies like artificial intelligence in its collection of that information.

The replacement for PIPEDA, drafted in the 44th Parliament as Bill C-27, wanted to give assessment powers to an internal data ombudsman and review power to a data protection tribunal when it involves commercial personal data, effectively cutting out the privacy commissioner.

The bill saw personal data as a business activity whose primary aim was to facilitate its movement to enhance a digital marketplace economy in Canada and abroad.

The bill also housed the controversial Artificial Intelligence and Data Act that offered very little privacy protection while promoting AI industries.

There is also talk of introducing legislation that would ban those under the age of 16 from social media while social media giants continue—without real regulation—to collect personal metadata from Canadians for market purposes.

Also waiting in the wings are the potential enabling rules for digital ID wallets where Canadians' personal information is brought together into one big digital tent.

But, through the now-passed 2025 budget bill C-15, citizens are allowed to move their data—welcomed by the private sector—between organizations.

Just introduced as part of the spring economic update is a proposed search-and-seizure measure allowing law enforcement agencies to open and detain Canadian's mail—with a focus on illegal contraband—to be shortly formalized as an amendment to the Canada Post Corporation Act.

Legislation restricting facial recognition technology, or other invasive technologies, has also not yet arrived.

There are already various federal-provincial territorial arrangements in play that affect privacy.

For instance, Treasury Board has—behind closed doors—been working on a Pan-Canadian Health Data Plan, that would reputedly "de-identify" collected and digitized personal data.

With all this legislation activity, how will individuals know the details of their information being used with advanced technologies and AI involved—and know when things go wrong?

Will there be more secret personal data files that Canadians know nothing about? What about more personal data manipulation that the acts underway do little to prevent?

Another underplayed aspect is that these initiatives are not well examined with costs and benefits known and debated.

For instance, there are large startup and annual costs that come with re-engineering electronic service provider systems to grant law enforcement agencies access to internet, telecom, or cloud subscribers' basic information.

Yet the government—as reported by the CBC on April 3—doesn't know how much those costs actually are.

The costs will be high, given a 2012 government estimate of $80-million attached to a then-proposed lawful access bill, as reported by the CBC on Feb. 22, 2012.

But with those installed surveillance systems having a limited shelf life, and being potentially vulnerable, is this police-sought re-engineering—that taxpayers will pay for—worth it?

And what do you do once costs lead to irregularities, cost overruns, and hidden costs?

An example of costly mistakes is the ongoing issue with the Phoenix pay system affecting many individuals whose shared personal information may or may not be correct.

Another example is the controversial ArriveCan advance border travel scheme that tracked individuals, and, at times distorted that information, which cost taxpayers an estimated $60-million—in part because of contract irregularities and hidden costs—against an initial $80,000 budget.

In the digital age, authorities are demanding more costly and questionable government and corporate surveillance, which is being legalized with limited self-policing, weaker internal monitoring, and limited regulation. But it comes with greater risks, including being open to abuse by domestic and foreign actors.

So, is anyone in government looking out for Canadians' privacy interests, especially now that Prime Minister Mark Carney has his majority government?

Who will stop the facilitation of further privacy incursions and violations?

Privacy protection continues to rate high in public polling. Yet recent legislative moves—likely accelerated with a majority government in place—are violating that trust, and invasively throwing rigorous personal data protection out the window.

Ken Rubin is a longtime privacy advocate and commentator reachable via kenrubin.ca.

The Hill Times

Link: https://www.hilltimes.com/2026/05/06/will-carneys-majority-government-usher-in-a-costly-era-of-privacy-invasion/502451/