

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p>Scope of Protected Information</p> <p>Canadian data protection law protects “personal information”, which is defined as “information about an identifiable individual.”⁴</p>	<p>The OEM Pledge defines “Identifiable Information” consistently with Canadian data protection law but fails to establish a clear threshold for determining when data is “not reasonably linkable” to an individual.</p>	<p>OEMs typically treat aggregated customer information that does not itself identify individuals as available for any use or disclosure, without specifying the risk of re-identification.</p>	<p>UBI providers define “personal information” as including all driving data that could be associated with the insured, whether or not the insured was driving at the time.</p> <p>Most UBI providers do not disclose their use of anonymized customer data to consumers, and none specify the ways in which data is anonymized or the risk of re-identification.</p>
<p>Openness and Accountability</p> <p>Commercial data processing activities must be transparent and available to the public. At a minimum, personal information management policies and practices must be easily and publicly accessible, generally understandable, and sufficiently detailed. Contact information for an individual responsible for the organization’s compliance must be provided (4.8, 4.8.1, 4.8.2).</p>	<p>The OEM Pledge fails to commit to openness and transparency as required by Canadian data protection law.</p>	<p>Most OEM Connected Car privacy policies applicable to Canadian consumers are not publicly available and cannot be reviewed without purchasing the vehicle or service.</p> <p>Some OEM policies are so incomplete, vague or open-ended in certain respects that they are unhelpful other than serving as a warning that the OEM does not respect consumer privacy.</p>	<p>Canadian UBI program providers are making relevant policy documents publicly available, allowing consumers to see and compare the degree of privacy protection each company provides.</p>

¹ Automakers, insurers and all other entities collecting, storing, using or disclosing personal data in the course of commercial activities are subject to *PIPEDA* or its provincial counterpart statutes. Insurers offering UBI in Canada are also subject to provincial industry regulation. Numbers after text refer to *PIPEDA* unless otherwise stated.

² *Commitment of the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. to the Consumer Privacy Protection Principles for Vehicle Technologies and Services*, November 12, 2014.

³ A non-comprehensive selection of major OEM Connected Car privacy policies publicly available online i

⁴ *PIPEDA* s.2; *AltaPIPA* s.1; *BCPIPA* s.1; *Quebec Act*, s.2.

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p><i>Accountability with respect to third party processors</i></p> <p>An organization is responsible for personal information in its possession or custody, including information that has been transferred or outsourced to a third party for processing (4.1.3).</p>	<p>OEMs fail to take responsibility for the use and disclosure of personal data they share with their affiliated dealers.</p>	<p>Most OEMs share customer data with dealers but do not require that their dealers provide comparable data protection.</p> <p>OEMs share customer data with wireless and other service providers, but do not always require that third parties provide comparable data protection.</p> <p>Some OEMS deny responsibility for privacy breaches by third parties to whom they entrusted customer data.</p>	<p>Canadian UBI programs acknowledge their responsibility for the data handling practices of their third party service providers in relation to personal information.</p>
<p><i>Individual Access to own data</i></p> <p>Individuals must be able to find out what information is held about them, how it is being used and to whom it has been disclosed (4.9.3.).</p>	<p>The OEM Pledge does not meet legal standards in Canada for individual access to personal data.</p>	<p>OEMs typically do not permit customers to find out what information about them has been shared with third parties for purposes other than service provision, nor do they offer to provide customers (other than California residents) with the names of third parties to whom customer data has been disclosed.</p>	<p>In addition to standard individual access rights, UBI providers typically allow customers to monitor their personal driving data collected via the telematics device.</p>
<p><i>Accuracy</i></p> <p>Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used (4.6).</p>	<p>Participating OEMs commit to “implementing reasonable measures to maintain the accuracy of Covered Information.”</p>	<p>OEMs have committed to taking reasonable steps to ensure accuracy of customer data.</p>	<p>UBI providers are subject to regulation requiring accuracy of the data on which they make insurance decisions about individual customers.</p>

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p>Security</p> <p>Personal information must be protected by security safeguards appropriate to the sensitivity of the information (4.7).</p>	<p>The OEM Pledge offers general assurances of data security in the provision of Connected Car services.</p>	<p>OEMs do not protect customer data according to a consistent set of industry standards, and there are serious questions about the adequacy of security measures they currently apply.</p> <p>Some OEMs expressly deny responsibility for security breaches by third parties to whom they have entrusted customer data.</p> <p>Some OEMs make customers responsible for any unauthorized access to or use of the services when appropriate user authorization has been provided, without explaining how the service has been designed to minimize the risk of unauthorized access or use.</p>	<p>Canadian insurers offer general assurances of data security in the provision of UBI.</p>
<p>Purpose Specification and Notice</p> <p>Organizations must identify and document the purposes for which they are collecting personal data (4.2). They must inform individual customers of the specific purposes for which their data is being collected(4.2.3, 4.3.2). New purposes require new customer consent (4.2.4).</p>	<p>The OEM Pledge commits to providing clear, meaningful notice in accordance with Canadian data protection law, but does not commit to bringing such notice to the attention of customers.</p>	<p>OEMs typically leave it up to customers to inform themselves of applicable privacy policies and of any changes to the policies.</p> <p>Some OEMs do not limit the purposes for which they collect, use and disclose customer data, allowing themselves to collect and use an unspecified amount of personal data for an unlimited range of purposes.</p>	<p>Canadian insurers offering UBI programs include detailed information regarding the specific types of personal information collected and the potential uses of that data.</p>

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p><i>Purpose Limitation</i></p> <p>An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (subsection 5(3)).</p>	<p>The OEM Pledge treats marketing, product development and improvement and internal R&D as non-optional purposes for which personal data may be used (and in the case of product development, improvement and R&D, disclosed).</p>	<p>Some OEMs do not limit the purposes for which they collect, use and disclose personal customer data.</p> <p>OEMs treat marketing and product R&D as appropriate purposes for non-optional collection of sensitive customer data.</p> <p>Some OEMs reserve the right to share sensitive customer data with unnamed third parties for marketing purposes, without offering an opt-out for customers.</p>	<p>Personal data collected for UBI purposes is not used or disclosed for any other purposes without express consent.</p>
<p><i>Limits on Collection</i></p> <p>Personal data must not be collected beyond what is needed for the (appropriate) identified purposes that have been communicated to customers and to which customers have consented (4.4, 4.4.1)</p>	<p>The OEM Pledge does not limit collection of personal data to that necessary for the purpose of the Connected Car services being provided.</p>	<p>OEMs justify the collection of vast amounts of personal data by improperly including marketing and other secondary uses in their non-optional purposes of collection.</p> <p>OEMs collect so much personal data for so many purposes that it is impossible to determine the extent to which they are collecting more data than necessary for each purpose without doing an audit.</p> <p>OEMs collect use personal data for purposes that could be accomplished using anonymized data.</p>	<p>UBI programs limit the collection of personal information to that necessary for insurance purposes.</p>

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p>Limits on Retention</p> <p>Personal information must not be retained longer than necessary to fulfil the (appropriate) purposes to which the customer has consented (4.4).</p>	<p>The OEM Pledge fails to limit the retention of personal data as required under Canadian data protection law.</p>	<p>OEMs retain customer data for secondary purposes such as marketing, and do so for as long as they decide is appropriate, without reference to any objective industry standards.</p>	<p>Specific information regarding retention of personal data is typically lacking in the privacy policies and terms of service of UBI providers.</p>
<p>Limits on Use and Disclosure</p> <p>Personal information must not be used or disclosed for purposes other than those for which it was collected, without the informed consent of the individual, or if required by law (4.5).</p>	<p>The OEM Pledge allows OEMs to use and disclose personal data of customers for unnecessary purposes without informed consent of customers.</p> <p>The OEM Pledge requires consent for the use of certain sensitive data for marketing purposes.</p> <p>The OEM Pledge requires consent for sharing of certain sensitive data with unaffiliated third parties.</p>	<p>OEMs use customer data for a wide range of sometimes vaguely worded purposes including marketing, R&D and other secondary uses, without clear customer consent.</p> <p>They also share customer data with third parties for a variety of sometimes vaguely worded purposes including marketing, without clear customer consent.</p>	<p>Canadian insurers limit uses and disclosures of personal information to the purposes for which it was collected.</p>

What Canadian privacy law requires ¹	OEM Pledge ²	Automakers' Policies ³	Usage-Based Insurance
<p><i>Informed Consent (Choice)</i></p> <p>Informed consent is required for all collection, use and disclosure of personal information (4.3). Consent can be implied where reasonable to expect that the individual is aware of the collection, use or disclosure and would agree to it if asked. Otherwise, consent must be obtained expressly. Opt-out consent is permissible in certain situations taking into account the sensitivity of the data and the reasonable expectations of the individual. Otherwise, affirmative, opt-in consent is required (4.3.4).</p>	<p>The OEM Pledge fails to require customer consent for even non-essential collection, use and disclosure of customer data, contrary to Canadian data protection laws.</p>	<p>OEMs claim implied consent by customers to the collection, use and disclosure of vast amounts of often sensitive personal data, for a wide range of purposes, many of which are not essential to provision of the services in question.</p> <p>With limited exceptions, OEMs do not allow customers to opt-out of listed uses or disclosures of their personal data even where such uses or disclosures are not essential to provision of the service. OEM policies do not provide sufficient detail for customers to understand the uses to which their personal data may be put.</p>	<p>Insurers obtain express, informed consent of customers to all collection, use and disclosure of customer data for UBI programs.</p>
<p><i>Refusal to Deal</i></p> <p>Companies must not require customers to consent to unnecessary data collection, use or disclosure (such as marketing or product improvement) as a condition of the supply of a product or service (4.3.3.).</p>	<p>The OEM Pledge violates the “refusal to deal” rule in Canadian data protection law except with respect to the use of certain kinds of customer data for marketing purposes and the sharing of such data with unaffiliated third parties for their own purposes.</p>	<p>OEMs often require that customers agree to unnecessary collection, use or disclosure of their personal data in order to register for Connected Car services.</p>	<p>No provider of UBI in Canada requires that customers consent to any non-essential collection, use or disclosure of their data in order to sign up for the UBI program.</p>

For more information, or to read the complete report: fipa.bc.ca/connected-car



BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

fipa@fipa.bc.ca
 103 - 1093 West Broadway
 Vancouver, BC V6H 1E2
 604.739.9788

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC). The views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.