On March 25, 2015, the BC Freedom of Information and Privacy Association (FIPA) released a report highlighting privacy challenges in something that rivals smartphones in ubiquity: cars. The 123-page report, entitled The Connected Car: Who’s in the Driver’s Seat?, examines the complex telematics systems found in cars nowadays that can do everything from unlocking doors, providing navigation, streaming music, reading your text messages, and calling your spouse to say you’ll be late. The number of features and sophistication of in-vehicle connectivity have grown in recent years and become a standard feature in vehicles of all makes and models. The report describes the large amounts of data that connected cars collect, some of which is personal and potentially sensitive, and the privacy and data security concerns surrounding the collection and use of this data.

The report analyzes the privacy policies of auto manufacturers and the Automakers’ Privacy Pledge of November 2014 (the “Automakers’ Pledge”) and assesses whether they comply with Canadian privacy legislation, namely the Personal Information and Protection of Electronic Documents Act (PIPEDA) and the substantially similar provincial legislation found in British Columbia, Alberta and Québec. The types of information that connected cars gather include information about driving habits, phone calls, location, vehicle statistics (distance travelled, airbag deployment, vehicle service status), browsing habits, personal contact lists, and users’ inputs and interaction with infotainment apps (such as music selection, search terms, and stored preferences). The information collected through connected cars is significant not only in its volume - the number of cars, and the significant periods of time that North Americans spend in their cars produces a high quantity of data - but in the potential for it to be combined and aggregated in ways to build highly personal and revealing profiles of users. The conclusion the report reaches is that carmakers are failing to meet Canadian privacy requirements in a number of ways, including:

- being vague and open-ended about the purposes of collecting personal information;
- requiring users to agree to information being used for “non-essential” purposes, such as marketing;
- treating anonymized or aggregated data as outside the scope of the privacy policy, without identifying the risks of re-identification;
- failing to disclose all the parties that information may be shared with; and
- deflecting responsibility for privacy compliance by referring to the separate privacy policies of third parties, such as the telecom companies that provide connectivity and app providers.

The report concludes with the recommendation that auto manufacturers create comprehensive Privacy Management Programs that provide oversight and review of privacy compliance. It also calls for government to enact new privacy and data protection regulations that are specific to the auto industry.

The report takes a serious misstep by choosing to analyze the Automakers’ Pledge, which was established by a US association of automakers for use in the US and not intended to apply in Canada. It is not clear why the author focuses on the Automakers’ Pledge when it is clearly presented as standards for the US market. There is a lack of empirical evidence that original equipment manufacturers (“OEMs”) have taken liberties with their privacy policies and actually used or disclosed personal information in ways that clearly contravene Canadian privacy laws. However, it is the suggestion that carmakers adhere to an industry-specific privacy code and, more specifically, one that applies to one particular feature in their cars, that is most problematic. PIPEDA was intended to impose uniform standards across industries, so prescribing specific rules for carmakers unfairly singles out the sector and creates a competitive disadvantage. Moreover, since telematics involves...
a network of OEMs, telecom providers, hardware and software suppliers, and others, a code would effectively apply to not only carmakers but an array of additional industries. The report’s specific suggestions for the privacy code would also hold the auto industry to a higher standard. For example, it is not clear that explaining the risks or re-identification of aggregate data is a requirement under PIPEDA, but the report wants to impose this on carmakers. The report also emphasizes the importance of collecting affirmative consent, which seems to undermine the fact that implied consent is permitted under PIPEDA and suggests that there are circumstances where it is categorically inapplicable when cars collect personal information.

The report tries to justify an industry-specific privacy code by drawing an analogy to motor vehicle safety standards, which are uniform across Canada. The answer to this is that we do have uniform privacy legislation in PIPEDA, and to suggest that we enact specific requirements for the auto industry is to undermine one of the legislation’s main goals and essentially re-write the rules.

AUTHOR

Adrian Liu
Toronto
416.367.6585
aliu@blg.com

INSURANCE AND TORT LIABILITY GROUP

National Leader
Lawrence Elliot
Ottawa
613.787.3537
lelliot@blg.com

Regional Leaders
Bruce Churchill-Smith
Calgary
403.232.9669
bchurchillsmith@blg.com

Stéphane Pitre
Montréal
514.954.3147
spitre@blg.com

T. Kirk Boyd
Ottawa
613.787.3563
kboyd@blg.com

Kevin A. McGivney
Toronto
416.367.6118
kmcgivney@blg.com

Graham Walker
Vancouver
604.640.4045
gwalker@blg.com

This publication is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser if you have specific questions or concerns. BLG does not warrant, guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP (BLG). If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to have your contact information removed from our mailing lists by phoning 1.877.BLG.LAW1 or by emailing unsubscribe@blg.com. BLG’s privacy policy relative to publications may be found at www.blg.com/home/website-electronic-privacy.