Privacy Impact Assessment
For
ICBC Telematics Pilot

Prepared by: Christina Ulveteg
Date: May 2019

Introduction

The Privacy Impact Assessment (PIA) has been developed to assist ICBC in meeting FIPPA requirements as well as to minimize privacy-related risks to both the individual and ICBC. The PIA is a risk management tool that assists ICBC in assessing, at the outset, the impact that a new or significantly modified program, process or practice, new or modified contract or information system (an "Initiative") may have on individual privacy. The end products of the PIA will be a high-level summary of the Initiative, a completed Risk Register, and recommendations in terms of any outstanding additional work required by the Initiative owner. For additional information, please see the PIA Guidelines located at http://thehub/WorkTools/WorkToolsDocuments/PIAGuidelines.pdf

Contact Information

Department/ Initiative Area		**Privacy & FOI Department**	
Name & Title:	Anne O'Brien Project Manager	Name & Title:	Christina Ulveteg Privacy Manager
Department:		Email:	Christina.ulveteg@icbc.com

Executive Summary

The Rate Affordability Action Plan (RAAP) aims to make insurance more affordable and fair for everyone by addressing rising claims costs including legal and vehicle repair costs, as well as improving rate fairness and promoting road safety. The Telematics Pilot is a project under RAAP.

ICBC is implementing a one year telematics pilot ("Pilot") to assess whether telematics programmes would have a positive impact on crash rates through incentivizing driving behaviour improvement. The Pilot will target inexperienced drivers who have 0 to 4 years driving experience. Personal information will be collected from these drivers, both directly and indirectly, as defined by FIPPA, s. 26. Therefore, both detailed notice and informed consent will be required to participate in the pilot. The goals of the Pilot are to understand the potential for telematics to:

- improve driver behaviour and reduce distracted driving resulting in fewer crashes,
- Improve the driving competency of Novice drivers (in BC's Graduated Licensing Program), and

- Deliver a positive customer experience that promotes safe driving.

In addition, the Pilot will obtain customer feedback on experiences, perceptions and attitudes as they relate to monitoring technologies.

For the Pilot, ICBC is working with Octo Telematics North America, LLC ("Octo") to provide a telematics device that couples with a phone application ("app"). Octo is a global insurance telematics provider with offices around the world and data centers located in Canada, USA, Italy, France and Ireland. Octo is a GDPR compliant organization. Personal information will be stored and accessed on servers at these locations, outside of Canada. Therefore, participants will have to consent to the storage and access of their personal information outside of Canada in accordance with FIPPA s. 30.1 (a).

Unquestionably, telematics raises implications about privacy therefore the careful management and earliest practical destruction of that location data forms a key feature of this Pilot's design and solution. Location data management and destruction within the Pilot is as follows:

- ICBC will not retain any geo-location data itself
- The geo-location data collected by Octo will be deleted across two of the three relevant Octo data centers ([redacted]) within seven days of receiving the geo-location data.
- On the third data center ([redacted] the geo-location data will be de-identified after seven days of receiving the information and permanently deleted at the conclusion of the Pilot.

Geo-location data is necessary for two key reasons within the Pilot:

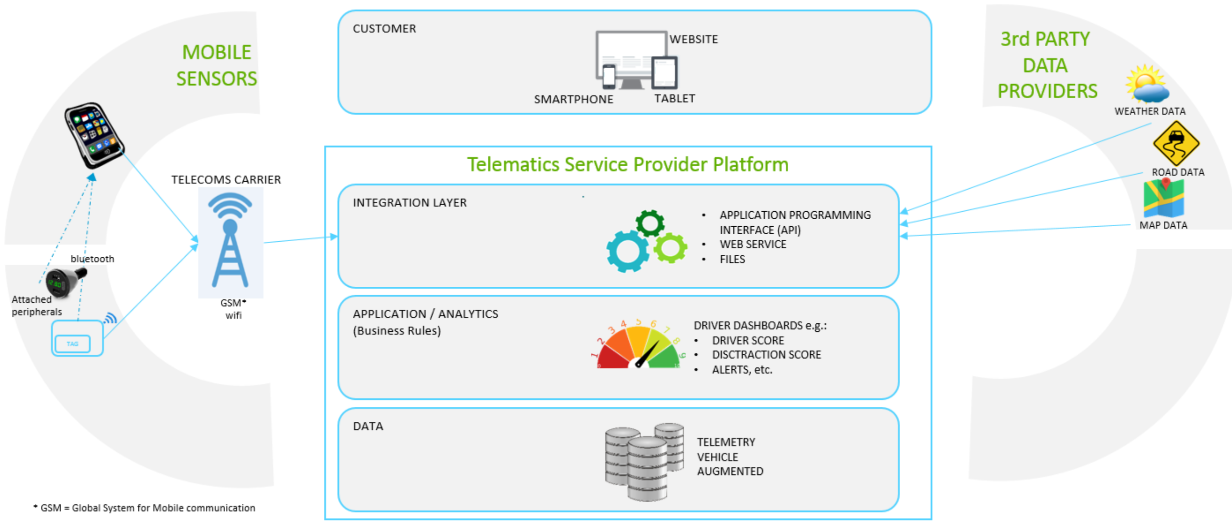
- Calculating speed and speed limit infringements, and
- Projecting driving events and distracted driving incidence to participants on a map-based view in the app.

Projecting events in context (on a map, in the case of telematics) is necessary for behavioural change. This assertion is confirmed by ICBC's customer research and a survey of research into the use of telematics to change driver behaviour. Feedback displayed on a map provides context and recall: It's the difference between simply knowing there was a severe braking event, versus knowing where the severe braking event occurred, which triggers the recall of the circumstances that led to the event. For these reasons, it is ICBC's position that the information to be collected meets the definition of "necessary" for the purpose of ICBC's program under FIPPA s. 26.

Background Information/Initiative Description

Overview of Telematics Architecture

Telematics systems produce data about vehicle operations, driver behaviours and vehicle location. Below is a high-level diagram of a generic telematics architecture.



In a basic telematics architecture, telematics data is created using devices or sensors that are onboard the vehicle. The data is transmitted to a telematics service provider's platform where a variety of processing activities may occur, such as data error cleansing, augmentation with third party data, and scoring the quality of trips and drivers.

The data may be fed back to the driver through a smartphone or web site. Depending on the nature of the particular telematics arrangement, the data may be passed on to an insurance company or fleet operator.

Insurers typically use telematics to attract low risk drivers, and to allow for better matching between price and risk. However the purpose of the Pilot is to assist ICBC in understanding the efficacy of telematics solutions to reduce crashes by providing feedback to drivers that will allow them to better understand and change their driving behaviour.

Unquestionably, telematics raises implications about privacy therefore the careful management and earliest practical destruction of that data is a key feature of this Pilot's design and solution.

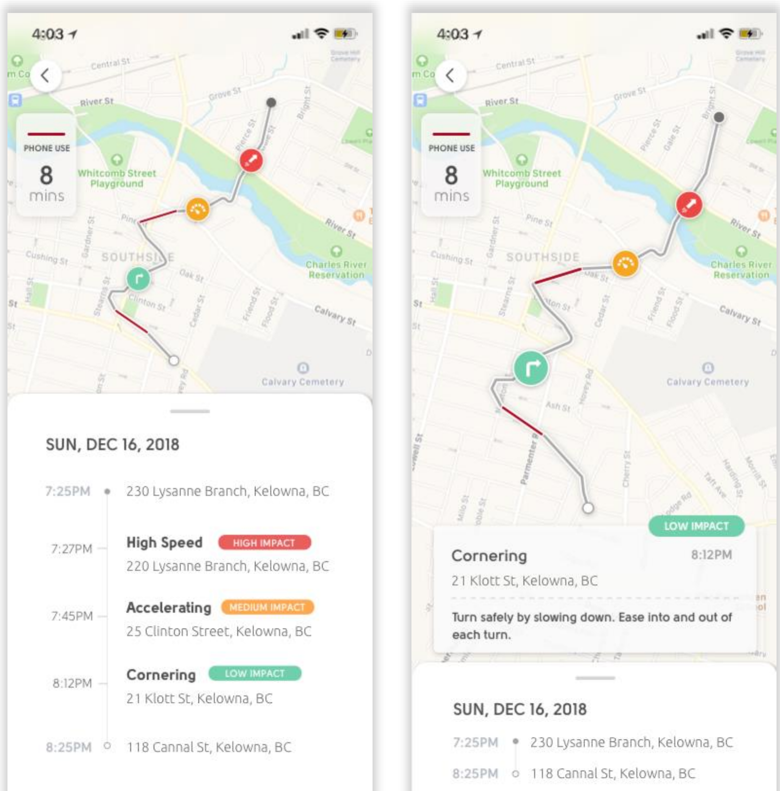
Overview of Octo's Telematics Architecture

Octo's telematics device, the "SmartTag", adheres to a vehicle's windshield and its phone app is called "Digital Driver". Digital Driver and the SmartTag are paired and calibrated via Bluetooth technology. Participation requires a smartphone (IPhone iOS 10 or higher, or Android 6.0 or higher) and a data plan.

The SmartTag comprises an accelerometer and a gyroscope, which are used to create telematics data about a participant's trips and driving behaviour. Since the SmartTag does not plug in to the vehicle's system it does not collect vehicle system information such as odometer, fuel level or engine health. The SmartTag does not cache any information.

[redacted].

The diagram (right) shows what the trip-based, map-based user interface looks like. Drivers can look through the last seven calendar day trip history and look at those trips on a map with driving events and distracted driving incidence flagged. Geo-location data is required to produce this user interface feature.



In addition to user interface trip mapping, the geo-location data is used to calculate both velocity and the data lookup to the third party road data to ascertain whether or not the driver was below the posted speed limit at the particular geo-location.

These speeding metrics are inputs to calculating trip scores and trip events. These metrics are calculated almost instantaneously, and once calculated the scoring/analytic system has no need of the geo-location data for further calculations. However, whereas the scoring/analytic system has only a temporary and short term need of the geo-location data, the user interface requires the information for longer, seven days, to give users content to engage with and reflect on their recent driving behaviour.

Overview of the Pilot

In 2019 ICBC intends to implement a 12 month Pilot with approximately 7,000 inexperienced drivers who have 4 years or less of driving experience. A large number of participants is required in order to detect statistically significant change in the crash rate between drivers using a telematics device and those who do not. The statistical target is a 95% confidence level and a margin error of 1.0%.

Participation in the Pilot is voluntary and there are no costs to the participants beyond phone data usage. Data usage is approximately the same amount as what running a navigation map tool like Google Maps would consume on a smartphone. Participants may withdraw from the Pilot at any time.

Currently, there is information on icbc.com about the Pilot as well as electronic signage information at Driver Licensing offices. When Pilot registration begins, ICBC will execute a marketing campaign in order to attract and recruit up to a maximum 7,000 participants. Prospective participants will register online through icbc.com.

Consent and terms and conditions acceptance will be captured as part of registering through icbc.com. Customers will agree to a single set of terms and conditions that govern all aspects of the pilot, including their subsequent download of Digital Driver. No separate consent will be required for the app download and use.

The participants will hold a class 5 or class 7N (Novice) licence and will be separated into two groups:

- A control group that will have the telematics technology installed but will not have access to Digital Driver's features and feedback, and
- A treatment group that will have the telematics technology installed and will have access to the Digital Driver's features and feedback.

Participants in the treatment group will be provided with a rich set of features to incentivize improved driving behaviour, whereas control group participants will not see these features. The main features that each group will see:

Feature	Treatment	Control
Pilot participation incentive	✓	✓
Recent trip paths (last seven days) listed and overlaid on map	✓	✓
Flagged events (such as speeding) listed and overlaid on map	✓	
Individual and aggregate trip scores	✓	
Individual and aggregate distracted driving scores	✓	
Gamification and challenges	✓	

Tips, alerts and education	✓	
Driving-based Rewards	✓	

The Pilot participation incentive and the driving-based rewards both come in the form of digital gift card of a variety of BC retailers and restaurants. Octo has subcontracted with Augeo Affinity Marketing Inc to provide the incentives and rewards. Digital Driver has a link to the Augeo shopping platform where participants can choose their digital gift card. The terms and conditions that the participant agreed to upon registration in the pilot will govern their use of Augeo's shopping platform. No separate consent will be required for Augeo.

The Pilot participation incentive is dispensed at appropriate time-based milestones throughout the Pilot. Driving-based rewards are earned throughout the Pilot by the participant tripping various "good driving" business rules and completing various challenges. The in-app incentive and rewards currency is diamonds. Participants receive diamonds that they can spend on the shopping platform.

Gamification comes in the form of opt-in leaderboard and challenges. The leaderboard will show the top 10 participant scores chosen username and relative ranking amongst all opted-in Participants.

ICBC will use the participant data, telematics data, and score data, as created and collected through the pilot, along with policy and vehicle information, participant crash history, chargeable claims and convictions history, to analyze the efficacy of the telematics services for improving driving behaviour and reducing crashes. Specifically, ICBC will compare the differences between the control group and the treatment group in their crash frequency, Driveability® Score, Distracted Driving Score, Driveability® score components, and various other behaviourial metrics such as average speed and average event count.

Personal Information Impacted by the Initiative

The diagram below shows the summary or high level data flow in the Pilot solution.

[redacted]

As summarized in the above diagram:

Participant Data is collected to determine Pilot eligibility, to analyze the Pilot's objectives, and for the service delivery of the Pilot (i.e. to ship SmartTags to customers). [redacted].

Telematics Data is created by the SmartTag and Digital Driver, and transmitted to Octo. It is used to both incentivize behavioural change through its projection on Digital Driver's map, and used to analyze the Pilot's objectives. [redacted]

Score Data [redacted]s. Similar to Telematics Data, it is used to both incentivize behavioural change through its visualization in Digital Driver, and used to analyze the Pilot's objectives. [redacted]t[redacted]

Game Data comprises the stars and diamonds created by the dispensing of the participation incentive and by accomplishing challenges and earning rewards. It also comprises the shopping history that Augeo accumulates on its sales platform (the use of which is to facilitate a smooth repeat-visit user experience). [redacted]

Principles governing the Pilot solution:

Necessary data flow: The only data that flows is the data required by the specific system it flows to. For example, a good portion of the **Participant Data** required in this solution never leaves ICBC. Only the essential elements of **Participant Data** are transmitted to Octo for the necessary functioning of Octo's systems. [redacted].

Minimized geo-location data accumulation: The solution has been designed to minimize geo-location data accumulation. [redacted] Geo-location data (part of the **Telematics Data** type) is stored in three locations, and each has a mechanism to manage geo-location data specifically:

- Digital Driver [redacted], [redacted] Deleted seven days after collection
  - [redacted]
  - The app UI will only look for the last seven days when looking at historical trips to load for each user.
- DriveAbility® ([redacted]) – Deleted seven days after collection
  - [redacted]
- Telematics Engine ([redacted]) – De-identified seven days of collection AND deleted at the conclusion of the pilot
  - [redacted]
  - In [redacted]
  - In addition to the seven-day de-identification, at the conclusion of the pilot the trip records in the trip data pool will be deleted [redacted].

Data retention and destruction: The overarching principle is to retain data within ICBC for a number of years (specified below) and to permanently delete data within Octo and Augeo. To retain data within ICBC means to capture the pilot data (other than geo-location data) as a data asset, in the form of both summary reporting (scheduled throughout the pilot) and detailed event and trip-level data to be retained in a data warehousing environment. This data asset is required to evaluate the Pilot's objective, "*Improve driver behaviour and reduce distracted driving resulting in fewer crashe*s", specifically to evaluate the "*improve driver behaviour*" component of that objective. To evaluate aggregated scores alone will not be a fulsome evaluation. A score is an abstraction of driving behaviour, therefore a fulsome evaluation is to evaluate both the score and the underlying driving behaviour data that produced the score.

The following personal information is collected, created, or used to facilitate both the delivery of the Pilot and the analysis of the Pilot objectives.

Situation	**Data Type**	**Data Fields**	**At-rest locations**	**Retention**
Collected by ICBC for the purpose of determining Pilot eligibility	Participant Data	• Driver's License Number • Plate number • Vehicle make • Driving experience in another jurisdiction • Confirmation of smartphone and a data plan	ICBC only	Retained within ICBC's system beyond the pilot duration for 5 years
Used by ICBC for the purpose of analysing the Pilot objectives	Participant Data	• Driver's License Number (identity key) • Plate number (identity key) • Any driver training history (differentiating factor)	ICBC only	Retained within ICBC's system beyond the pilot duration for 5 years
Collected by ICBC and provided to Octo for the service delivery of the Pilot	Participant Data	• First and last name • Valid email address • Mobile phone number	ICBC [redacted]	ICBC: Retained within ICBC's system beyond the pilot duration for 5 years Octo: Deleted within the pilot duration. Service support information deleted at pilot conclusion.
Collected by ICBC and provided to Octo for the shipping of SmartTags to customers	Participant Data	• First and last name • Mailing address	ICBC [redacted]	ICBC: Retained within ICBC's system beyond the pilot duration for 5 years Octo: Deleted within the pilot duration. Shipping information deleted when shipping complete.

Situation	Data Type	Data Fields	At-rest locations	Retention
Created by ICBC and provided to Octo for the service delivery of the Pilot	Participant Data	• Participant's status as Treatment or Control • Unique participant ID	ICBC [redacted]	ICBC: Retained within ICBC's system beyond the pilot duration for 5 years Octo: Deleted within 3 months of the pilot conclusion.
Collected by Octo for the service delivery of the Pilot	Participant Data	• Smartphone serial number (IMEI)	[redacted]	Octo: Deleted within 3 months of the pilot conclusion.
Telematics data as created by the SmartTag and Digital Driver, and transmitted to Octo [redacted]	Telematics Data	• Geo-location as recorded by the GPS • Time stamp • Distraction events (for example, that the smart phone was in use but not which apps or phone features were accessed) • Accelerometer and gyroscope data including participants acceleration, deceleration, cornering g-force and compass heading • Whether participants have indicated that they were NOT the driver of a trip that was recorded • Participants usage interactions with Digital Driver	[redacted]	ICBC: Transmitted from Octo to ICBC, without geo-location, aggregated to event-level and trip-level reports, and retained within ICBC's system beyond the pilot duration for 8 years. Octo: • Digital Driver [redacted] Deleted seven days after collection • DriveAbility® [redacted] [redacted] – Deleted seven days after collection • Telematics Engine [redacted], [redacted] De-identified seven days after collection AND deleted at the conclusion of the pilot

Situation	Data Type	Data Fields	At-rest locations	Retention
Telematics data as created or calculated by Octo	Telematics Data	• When trips occur including both starting and stopping (date and time of day) • The amount of time travelled • The distance driven in km • Participants speed of travel and average speed as inferred by the GPS • Road conditions [not personal information] • Weather conditions [not personal information] • Traffic [not personal information]	*As above*	*As above*
Scoring data as created by Octo Scoring data is maintained on a: • Per-trip and rolling 100 day basis for the purpose of feeding back to Digital Driver, and • Cumulative basis for the purpose of analysing the Pilot objectives.	Scoring Data	• DriveAbility® Score • DriveAbility® Score Component Distance • DriveAbility® Score Component Smoothness • DriveAbility® Score Component Time Of Day • DriveAbility® Score Component Roads • Distracted Driving Score	[redacted]	*As above*
Collected by Octo for the purpose of providing a "gamified" customer experience	Game Data	• Participant profile icon • Participant screen name	[redacted]	Deleted within 3 months of the pilot conclusion.

Situation	Data Type	Data Fields	At-rest locations	Retention
Created by Octo and provided to Augeo for the purpose of providing rewards and the participation incentive	Game Data	• Rewards and pilot participation points (stars and diamonds, as virtual currency)	[redacted]	ICBC: Transmitted from Octo to ICBC as event-level reports, and retained within ICBC's system beyond the pilot duration for 8 years. Octo: Deleted within 3 months of the pilot conclusion. Augeo: Deleted within 3 months of the pilot conclusion.
Collected by Augeo for the purpose of digital gift card delivery and any follow-up customer service required.	Participant Data	• Name • Phone Number • Email address	[redacted]	Collected by Augeo on the first reward redemption transaction Deleted within 3 months of the pilot conclusion.

FIPPA Compliance Analysis

Collection (s.26)

Section 26 of FIPPA outlines when personal information may be collected by a public body (ICBC is a public body). Section 26 is applicable.

For the Pilot, the information will be collected under sections 26 (c), and (e), which state:

> **26** A public body may collect personal information only if
> …
> (c) the information relates directly to and is necessary for a program or activity of the public body,
> …
> (e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

Section 26 (c) contains a two part test and both parts need to be met before information can be collected under this section. Specifically, the information must be: (1) directly related to a program or activity of the public body, and (2) necessary for the program or activity.

One of ICBC's legislated functions is to "promote and improve highway safety"[1] and in order to do so it is specifically given the power to "promote or carry out programs of research into causes of accidents and the equitable distribution of losses resulting from highway traffic accidents"[2] . The purpose of this pilot is to evaluate the road safety benefits of a telematics program, which fits within ICBC's road safety mandate. In addition, this legislated mandate clearly links ICBC's insurance business with its road safety portfolio. Therefore the information collected for the Pilot is directly related to ICBC's programs, which meets the first part of section 26(c),

The second part of 26(c) (and also found in s.26(e)) is that the information must be necessary for the program or activity of the public body. In Order F07-10, former Commissioner Loukidelis considers the definition of "necessary" and states:

> [49] At the same time, I am not prepared to accept, as the Complainants contend, that in all cases personal information should be found to be "necessary" only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is "necessary" even where it is not indispensable in this sense. The assessment of whether personal

[1] Insurance Corporation Act - Section 7(j)
[2] Insurance Corporation Act - Section 9(j)

> information is "necessary" will be conducted in a searching and rigorous way. In assessing whether personal information is "necessary", one considers the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA's privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.

Applying the reasoning set out above, we would first look at the sensitivity of the information in question. Some of the information being collected for this pilot is geolocation information which, when combined with other personal information about an individual can be considered sensitive. Because of this, tight security controls are in place to protect this information. Personal information will be encrypted both in transit and at rest. Other security controls are discussed further in the security section of this PIA and in the Information Security Risk Assessment (Appendix A).

With respect to the purpose of the information collected, it would allow ICBC to determine if telematics have an impact on improving driving behaviour for inexperienced drivers and in reducing crash rates. Without this information, ICBC would not be able to make this assessment, and successfully achieve the Pilot goals. Geo-location data collected is used to provide participants with integral feedback that plots trip events on a map within the Digital Driver application. Participants will be able to view trips taken, and see a map view on Digital Driver along with other information regarding their driving. Geo-location data is also required to generate the speeding component of the scoring and feedback. Without this context, the likelihood of affecting the desired behaviour change is severely limited.

The goal of the Pilot from a user experience perspective is to understand and improve driving behaviours. The feedback with mapping context provided through the application enables a customer to consume, process and utilize the information. This is because the visual context makes the difference between a driver knowing how they drive, and knowing how they can improve their driving. The geolocation data allows drivers to know the 'where' of driving events; the 'where' informs the 'why', and the answer to 'why' leads to understanding. Without the geo-location and map view, it is unlikely the goals of the Pilot would be achieved.

ICBC conducted its own customer research on whether having the geolocation information was useful (Appendix B). The overall response from the participants was that having the geo-location information was important and impacts the ability of drivers to recall instances of their unsafe driving. In addition, ICBC conducted a literature review on the importance and implications of presenting information in context (Appendix C).

While the amount of information collected is not insignificant, it is considerably smaller during the course of the pilot than it would be if ICBC were launching a fully developed program. In addition, participation in the pilot is fully voluntary and participants will be fully informed via written documentation and consent forms of how their information will be used, accessed, disclosed, and later destroyed.

It is ICBC's position that for all of the reasons set out above, the information being collected meets the definition of "necessary" for the purpose of ICBC's program under s. 26. Therefore the second part of section 26(c) is met.

Section 26(e) authorizes the collection of personal information for the purposes of planning or evaluating a program of a public body. It is important for public bodies to be able to conduct pilots in order to determine the viability of any new program before undertaking programs on a larger scale or seeking legislative amendments. Without this ability, it would be impossible to determine whether a program is viable without having a wide reaching impact on large populations. Further, by doing a pilot, the amount of personal information collected is limited in scope (7,000 participants as compared to the 3.5 million total active BC licenced drivers).

Currently, the only information being collected is the first & last name and the email address of interested drivers who wish to receive updates about the Pilot. This information is necessary to contact interested drivers with updates about the Pilot (s.26 (c)).

Additional personal information as outlined will be collected when the Pilot goes live and ICBC commences participant recruitment. When participants enroll online in the Pilot, the personal information will be collected under sections 26 (c) & (e).

Whenever data is collected a potential risk is that more information may be collected than is needed. For the Pilot, only the necessary amount of personal information will be collected to effectively conduct the pilot, which aligns with the best practice of only collecting the minimum amount of personal information to achieve the business purpose.

Notification (s.27)

As required by FIPPA, when collecting personal information, it must be collected directly from the individual unless another circumstance listed under section 27(1) applies. For the Pilot, personal information will be collected directly and indirectly. Informed consent will be required to participate in the pilot.

Pursuant to s. 27(2) of FIPPA whenever personal information is collected from an individual they should be informed of the following: (a) the purpose for collecting it, (b) the legal authority for collecting it, and (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Currently, the following notice is on the icbc.com page where interested drivers can sign up to receive updates on the Pilot:

> Personal information on this form is collected under s.26 of the *Freedom of Information and Protection of Privacy Act* and will be used for the purpose of contacting you in the future about the telematics pilot. If you have any questions about the collection of information, please contact us.

Applicable future notices and consents will be developed, as required, so participants in the Pilot will understand the purpose(s) of the Pilot's collection and the relevant authorities.

Use

Section 32(a) of FIPPA states that a public body must ensure that personal information in its custody or under its control is used only for the purpose for which that information was obtained or compiled, or for a use consistent with the purpose. Section 34 defines consistent purposes as (a) has a reasonable and direct connection to that purpose, and (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information or causes the information to be used or disclosed.

The data collected through the Pilot will be used to understand driver behaviour and to determine if the use of telematics reduces crashes.

ICBC will pair the Driveability® score information and distracted driving score information with participant policy information, vehicle information (VIN), crash history, chargeable claims, and convictions history to analyze the efficacy of the telematics services. Existing information from claims, insurance and driver licensing systems will be used. Participants will be providing their consent for the use of this information (s. 32(b)).

Geo-location data will be used in the service delivery of the pilot only. Participants will be able to view trips taken, see a map view on Digital Driver along with other information regarding their driving. Geo-location data is also required to generate speeding metrics and speeding events. Geo-location data is sensitive information, particularly when accumulated over time. Therefore ICBC will not retain any geo-location data itself and the geo-location data on Octo's side will be deleted across two of the three relevant Octo systems ([redacted]) within 7 days of receiving the geo-location data. On the third system [redacted] the geo-location data will be de-identified after seven days of receiving the information and permanently deleted at the conclusion of the Pilot. In addition, since Octo is GDPR compliant, its data operations and repositories are structured in a distributed, tokenized manner whereby it is deliberately difficult to recompile or re-contextualize a driver profile or trip list from any one location within the Octo system landscape.

The above controls will help mitigate any potential inherent risk the data collected for the Pilot will be used of other unintended uses.

Disclosure

Section 33 states that a public body must ensure that personal information in its custody or under its control is disclosed only as permitted under section 33.1 (inside or outside Canada) or 33.2 (inside Canada only).

ICBC does not intend to disclose personally identifiable information from the pilot.

Any requests from a participant for information pertaining to themselves would be processed and disclosed in accordance with part 2 of FIPPA.

For any third party data requests, ICBC would not disclose any individual telematics or participant personal information.

Disclosure of data to law enforcement under FIPPA is in the discretion of the public body under s. 33.2(i), and it is not ICBC's intention to disclose telematics or location data from this pilot to law enforcement.

ICBC will not disclose personal information from the Pilot to any operationalized process within ICBC. For example, the information will not be used to underwrite insurance or adjust claims.

Security

Section 30 of FIPPA requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

The level and type of security measures built into a system depend on the nature and sensitivity of the personal information the system will use and store.
The following security information about Octo is from information Octo provided on Form 9 – Security Questionnaire for NRFP 2018 and the information security risk assessment conducted by ICBC's information risk management team. This PIA sets out the security at a very high level. More detail can be found in the Information Security Risk Assessment itself (Appendix A).

Physical security of Octo Data Centers

All Octo Data Centers Server Rooms and offices are physically protected. The systems are located in specific Data Center Tier 4 facilities, whose access is regulated by a strict authorization process.

Access to Octo offices and facilities is managed through a company badge, which is provided to all employees and external collaborators. There is an intruder detection system that runs overnight and during weekends. Octo Headquarters physical security is controlled by remote surveillance performed by Security Service remote control room and night patrol control.

Access controls

Octo has specific policies and procedures in place to establish processes and work flows for Access Management.

User profiles and access privileges are assigned and authorised according to role and responsibilities, and are kept up-to-date with respect to the relevant changes.

The rights and roles concept for internal employees and contractors is based on the need to know and least privileges principles. Segregation of duties is applied with specific profiles as outlined in the Information Security Risk Assessment (Appendix A).

Access rights to information and information processing services are removed for all employees and external party users, upon termination of their employment, contract or agreement.

Network security controls

Octo is an ISO 27001 certified organization. Octo has established and implemented controls to ensure the security of information in networks and the protection of connected services from unauthorised access. Security measures are in place, such as: DMZ areas; Firewalls with anti-botnet protection; and Anti-malware systems.

Network and system segmentation techniques (such as VLANs, firewalling, virtual hosts) allow each customer to have a dedicated environment that is physically or logically segregated from the other. An IRM security risk assessment has been conducted and the overall residual security risk level has been identified as: Moderate.

Storage, Access & Retention

Under section 30.1 of FIPPA all personal information must be stored and accessed in Canada unless FIPPA authorizes otherwise.

While FIPPA generally prohibits the storage or access of personal information outside of Canada, there are certain circumstances where it is authorized. For the Pilot, personal information will be stored and accessed on servers located outside of Canada. Therefore, participants will consent to the storage and access of their personal information outside of Canada in accordance with section 30.1 (a).

All policy, claims, vehicle, drivers licensing, and convictions data used within the Pilot will be stored on ICBC servers in Canada.

Octo will store participant personal information on servers located in Canada, in the United States of America, and in the European Union (Italy, Ireland, and France). Augeo will store participant information on servers located in the United States of America.

The consent form will be comprehensive and will include all the requirements outlined in s. 11 of the FIPPA regulations.

A privacy best practice is to only retain personal information for as long as needed to achieve the business purpose. If personal information is stored for longer than necessary then there is the potential risk for inaccuracy of the information, unauthorized access and/or disclosure of the personal information.

Once the pilot has concluded, ICBC will analyze the data and retain it for a total of 8 years. It will be retained for 5 years identifiable and a further 3 years de-identified. The data when stored on ICBC's system will be segregated from other ICBC data. ICBC will not retain any geo-location data itself and the geo-location data on Octo's side will be deleted across two of the three relevant Octo systems ([redacted]) within 7 days of receiving the geo-location data. On the third system [redacted] the geo-location data will be de-identified after seven days of receiving the information and permanently deleted at the conclusion of the Pilot.

<u>Other FIPPA Considerations</u>

Data Linking Initiative:

"Data linking" is defined as: "the linking or combining of personal information in one database with personal information in one or more other databases if the purpose of the linking or combining is different from:

(a) the purpose for which the information in each database was originally obtained or compiled, and

(b) every purpose that is consistent with each purpose referred to in paragraph (a)".

A "**data-linking initiative"** is defined as: "a new or newly revised enactment, system, project, program or activity that has, as a component, data linking between

(a) two or more public bodies, or

(b) one or more public bodies and one or more agencies."

1. Personal information from one database is linked or combined with personal information from another database; information from claims, insurance and driver licensing will be used in the Pilot	yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

- ***This is not a data linking initiative.***

Common or integrated program/activity:

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no

- ***This is not a common or integrated program or initiative.***

<u>Privacy Risks Identified & Assessed</u>

The following privacy risks have been identified:

- Risk that more information will be collected than necessary for the pilot
  - For the Pilot, all the personal information identified is necessary and useful for program design purposes.

- Risk that the personally identifiable data collected will be used for other purposes.
  - Any other use of personally identifiable data will be assessed to ensure it is authorized under FIPPA. This risk does not apply to aggregated data.

- Risk that personal information will be stored and accessed outside of Canada without authority
  - Consent will be obtained from participants to store and access their personal information outside of Canada (section 30.1(a) of FIPPA)

- Risk that data will be stored for longer than necessary.
  - ICBC will retain the data for a total of 8 years after the pilot. After 5 years, the pilot data will be de-identified. ICBC will not retain any geo-location data

- Risk of unauthorized disclosure by the vendor
  - Vendor, as a service provider, will be subject to the requirements of FIPPA. In addition, any agreement with the vendor will have obligations regarding the protection of personal information. Vendor is GDPR compliant.

PIA Conclusion/Proposed Action Plans

The collection and use of personal information for the Pilot is authorized under FIPPA.

The Pilot is voluntary, of short duration and participants may withdraw at any time. Participation in the Pilot will have no impact on an individual's insurance or driving record.

The overall Privacy residual risk for this initiative is Moderate.

The Business Owner/PM is responsible to notify PFOI of any material changes to scope so a re-assessment can be completed.

Approval (residual risk basis)

The PIA approval process utilizes a **risk based approach** which ensures the final approval authority is commensurate with the complexity of the initiative and the degree of residual privacy risk remaining after implementation of any recommendations. In exceptional circumstances, the signing authority may be elevated.

Approval of this PIA by PFOI indicates acceptance of accountability for the methodology and analysis employed in this assessment.

Approval of this PIA by the Line of Business indicates acceptance of accountability for the accuracy of the information provided to PFOI for this assessment and accountability for implementation of the mitigation efforts outlined in the PIA Risk Register below.

Acceptance of the **residual risk** on behalf of ICBC is to be in accordance with the corporate Risk Measures Accountability and Risk Acceptance Authority Matrix http://thehub/WorkTools/WorkToolsDocuments/crm_framework.pdf

Legend:	Risk Ranking	Risk Acceptance Authority
Extreme	(16-25)	• Only the CEO has authority to accept **Extreme** residual risk with endorsement by the Board Committee assigned to monitor the particular risk.

High	(10-15)	• Only the ELT risk owner has authority to accept **High** residual risk with endorsement by CEO.
Moderate	(5-9)	• SLT risk owners and/or Divisional Risk Champion(s) have authority to accept **Moderate** residual risk with endorsement the ELT risk owner.
Low / Nil	(1-4) or NIL	• OLT risk owners have authority to accept **Low** risk with endorsement by the SLT and/or Divisional Risk Champion.

Approved by:

ORIGINAL SIGNED BY

Nicola Linton
Privacy & FOI Manager

ORIGINAL SIGNED BY

Myrthee Blanco
Senior Director Product & Customer Strategy

ORIGINAL SIGNED BY

Bill Carpenter
Vice President, Insurance

ORIGNAL SIGNED BY

Jason McDaniel
Vice President, Corporate Affairs

PIA Risk Register: Privacy-related risks are identified using ICBC's corporate risk assessment methodology

(For further details and definition, please refer to the Corporate Risk Measures: http://thehub/WorkTools/WorkToolsDocuments/CorporateRiskMeasures.pdf)

		Inherent Risk					Residual Risk							
Risk Type	**Describe risk, privacy impact or issue**	**Impact (NIL-5)**	**Likelihood (NIL-5)**	**Risk Score (I X L)**	**Risk Level (L,M,H)**	**Key Controls**	**Impact (NIL-5)**	**Likelihood (NIL-5)**	**Risk Score (I X L)**	**Risk Level (L,M,H)**	**Action Plan** (Avoid, Mitigate, Transfer or Accept)	**Action Plan Details**	**Follow up Date***	**Project/business area actions & response**
Reputation/ Legal	Risk that more information will be collected than necessary for the pilot	3	3	9	M	App and beacon will be configured so that only data necessary for evaluation of the pilot will be collected	3	2	6	**M**	Accept			
Legal	Risk that the personally identifiable data collected will be used for other purposes.	4	3	12	H	Data for this pilot when stored on ICBC's system will be segregated from other ICBC data. ICBC will retain the data for a total of 8 years after the pilot. After 5 years, the pilot data will be de-identified. ICBC will not retain any geo-location data itself and the geo-location data on Octo's side will be deleted across two of the three relevant Octo systems ([redacted]) within 7 days of receiving the geo-location data. On the third system [redacted] the geo-location data will be de-identified after seven days of receiving the information and permanently deleted at the conclusion of the Pilot. S. 32 of FIPPA prohibits supplementary use of data.	3	2	6	**M**	Accept			
Legal	Risk that personal information will be stored and accessed outside of Canada without authority	5	5	25	E	Consent will be obtained under section 30.1(a) from participants to store and access their personal outside of Canada.	4	1	4	**L**	Accept			

		Inherent Risk					Residual Risk							
Risk Type	**Describe risk, privacy impact or issue**	**Impact (NIL-5)**	**Likelihood (NIL-5)**	**Risk Score (I X L)**	**Risk Level (L,M,H)**	**Key Controls**	**Impact (NIL-5)**	**Likelihood (NIL-5)**	**Risk Score (I X L)**	**Risk Level (L,M,H)**	**Action Plan** (Avoid, Mitigate, Transfer or Accept)	**Action Plan Details**	**Follow up Date***	**Project/business area actions & response**
Reputation	Risk of unauthorized disclosure by the vendor	5	3	15	H	Vendor uses business rules (roles and permissions) using the principles of least privilege and need to know. In additional the Vendor is subject to the requirements of the contract and the legislative requirements of FIPPA.	5	1	5	**M**	Accept			

APPENDIX A – INFORMATION SECURITY RISK ASSESSMENT

NOT INCLUDED FOR SECURITY PURPOSES

APPENDIX B – ICBC CUSTOMER RESEARCH

Telematics Pilot

Mobile App Geolocation A/B Test Results

3 May 2019

DRAFT | Confidential

Observations

Participants liked the application and thought it would help encourage safe driving. In particular, they believed having map functionality would be key in aiding them in recalling a particular driving event.

- "The map helps me visualize where the event happened."
- "The version without the map wouldn't be helpful remembering the events"
- "These days, people have high expectations about the details"
- "one of the main benefits of the version with a map is when I am driving high speed in a school zone (even if I didn't notice at the time of driving)… When I refer to the map, the information is there for me as a reminder. So, this information will help me in the future to be careful when I am driving in school zone."
- "The version with the map is so much better and definitely helpful"
- "I can remember that (event) a lot more if I can tell where it happened then I can picture it a lot better"

DRAFT | Confidential 2

Recommendation

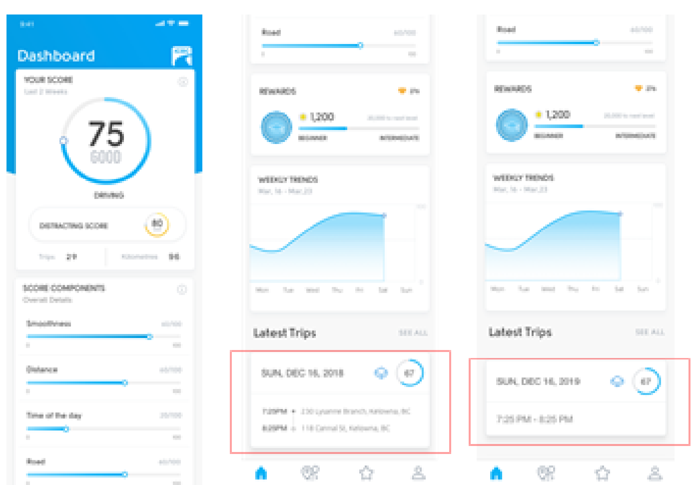
The overwhelming response by our test participants reflects our belief that providing location information greatly impacts the ability of drivers to recall instances of their unsafe driving. Not supplying this information reduces both the effectiveness of being able to effect behaviour change over time, and also removes a key element to keeping people using the device and app to track their driving habits.

Driving is not a one time event; habits are changed over time. Removing map functionality severely impacts the contextual reflection required to change the poor behaviours they we alerted to. People make decisions by recalling what they did last time using contextual information. By helping them recall the context in which a poor driving decision was made, user are more likely take corrective action, especially when they can specify how, when, and where. Removing geolocation removes the "where."

We recommend retaining the geolocation information used by the telematics application to reinforce safe driving behaviours.

Test prototypes

Dashboard



With location data

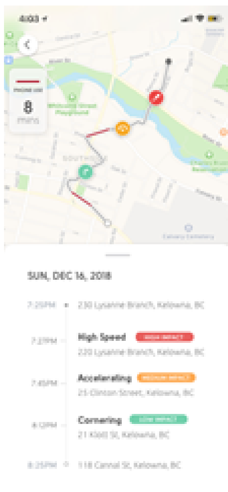
Without location data

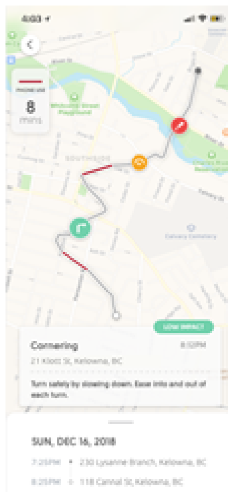
Observations:

- Dashboard screen is used as entry way to the more detailed trip information
- Users clicked through to the next screen without issue

Test prototypes

Trip Details with location data





Observations:

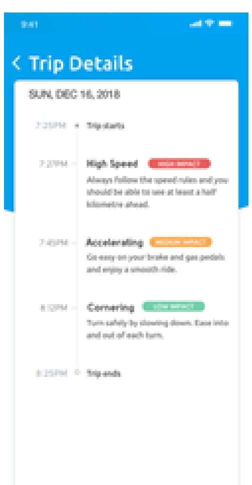
- A frequent request would be to include street-level images to help jog their memory as to the location and circumstances of the unsafe driving event.

DRAFT | Confidential

5

Test prototypes

Trip Details without location data



Observations:

- 4 of the 5 users presented this version first said they would not likely be able to remember a specific unsafe driving event given only this information. The 1 other user said they think they could but including a map would be helpful.
- When asked if adding anything else would aid in recalling an unsafe driving event, 4 of the 5 users presented this version first said that adding a map (or link to Google Maps) would help them

DRAFT | Confidential

6

Usability Ratings

	Version with the map	Version without the map
Which version did you find easier to use?	9	1
Which version would help you recall the events that happened on your trip more easily?	10	0
Which version did you prefer?	10	0

For the version with the map how comfortable are you with seeing your trip information stored in the app? Note that ICBC does not receive any personal identifiable information about an individual's trip. Any location information ICBC receives is anonymized and summarized as trends.

Very comfortable	Slightly comfortable	Slightly uncomfortable	Very uncomfortable
7	3	0	0

DRAFT | Confidential 7

Usability Ratings

Why did you prefer that version? (The version with the map)

- "It had an additional visual to recall memories. The time by itself is not necessarily going to help with remembering when the event occurred"
- "Easier to remember where possible incidents happened."
- "More attention to detail. Allowed me to visually see what was going on and what I can fix for the future."
- "More accuracy"
- "in map version if you over speed in certain areas again and again you will know where I am over speeding."
- "Easier to determine where I made specific errors on the road and to prevent the same incident from occurring in the future."
- "having the map I think helps you remember your trip more accurately"
- "Context helps with recall greatly"
- "it helped me visualize the areas that I should be cautious in."
- "I am a visual person and I like to see where I have traveled. I find it makes it easier to recall events if I have a map."

DRAFT | Confidential 8

Usability Ratings

Do you have any additional comments?

- "The point system is very interesting and I encourage the advancing of this project. I think this will help encourage safe driving in BC"
- "Beneficial"

Methodology

Sessions

To determine the users' reaction to the two versions of the mobile application (with and without the map), and address the ability of the application to assist the users in recalling instances of unsafe driving during their trips.

Sessions occurred at a ICBC Driver Licensing office in Port Coquitlam, on May 1st, 2019.

Scenario

"You have signed up for an experimental pilot with ICBC on safe driving where you have put ~~in~~ a device in your car to help measure how good your driving is on a daily basis. You can also earn points when you drive well and use these points to redeem prizes. To show your driving score, your points and other data about your driving, you have installed an app on a phone the device pairs with ~~it~~ so that you can see how you are doing. Today, we want to test two different versions of a part of that app."

Methodology

Tasks

(Group A would test with map first, without map second; Group B would test without map first, with map second)

1. Take a look at your driving score.
2. If you scroll down, you'll see a list of the trips that recently affected your score
3. Click on this trip *(ask them to pick the one we built on)*
4. Describe to me what you think this screen is doing.
5. Point out a particular event *(hard cornering one)*
6. Do you think with this information, you would likely be able to remember what happened in that particular event if it really happened?
7. Is there anything else on this screen we can add that would help you remember what happened?

After question

Compare and contrast the two different screens. Which one did you like better? Why?

Participant Demographics

A total of 10 ICBC customers participated.

Participant	Gender	Age range	Is English your primary language?	Years of Driving Experience	How often do you use apps on your phone?
1A	Male	16 – 24	Yes	1 – 4	Often / All the time
2A	Male	16 – 24	Yes	1 – 4	Often / All the time
3A	Male	16 – 24	Yes	1 – 4	Often / All the time
4A	Female	16 – 24	Yes	1 – 4	Often / All the time
5A	Male	16 – 24	No	1 – 4	Never, I just use my phone for calling
1B	Male	16 – 24	Yes	1 – 4	Often / All the time
2B	Female	16 – 24	Yes	1 – 4	Often / All the time
3B	Female	25 – 39	Yes	10 – 14	Sometimes
4B	Female	16 – 24	Yes	1 – 4	Often / All the time
5B	Female	40 - 69	Yes	15+	Often / All the time

APPENDIX C – ICBC LITERATURE RESEARCH

Geo-location data collected is used to provide participants with integral feedback that plots trip events on a map within the Digital Driver application. Participants will be able to view trips taken, and see a map view on Digital Driver along with other information regarding their driving. Geo-location data is also required to generate the components of the scoring and feedback. Since traditional driver feedback methods cannot be tailored to personal needs, they may not have the desired long-term influence on driving behaviour.[3] Therefore without the context provided by geo-location data, the likelihood of affecting the desired behaviour change is very limited.

Improving driver behaviour

The goal of the Pilot from a user experience perspective is to understand and improve driving behaviours. The feedback with mapping context, provided through the application, enables a customer to consume, process and utilize the information. This is because the visual context informs a driver not just about how they drive, but about how they can improve their driving: it enables drivers to learn what unsafe driving is, how to act in particular situations, and whether their driving has improved from previous trips.[4] Feedback with mapping context allows drivers to know the 'where' of driving events; the 'where' informs the 'why', and the answer to 'why' can provide enough information to facilitate behavioural change.[5]

For example, geo-location data allows a driver to see the same type of event mapped several times in the same spot, such as multiple speeding events that all occurred in a school zone. Identifying such recurring behaviour patterns helps to achieve the goal of long-term behaviour change.[6]

Feedback displayed on a map provides context to high-risk events; it's the difference between simply knowing there was a severe braking event, for example, versus seeing there was a severe braking event at a specific location. The additional level of information triggers the driver's memory of a the trip, which is required to change the feedback from basic information to something that facilitates self-assessment and learning[7]: 'I remember that the light changed at that intersection, so the driver in front of me braked but I was distracted so I had to slam on my brakes to avoid a collision'. Without this memory trigger, drivers cannot be as effectively alerted to unsafe behaviour such as speeding, lane departure or following the car in front of them too closely.

---

[3] Feng, Jing and Donmez, Birsen. Design of Effective Feedback: Understanding Driver, Feedback, and their Interaction. In: Proceedings of the Seventh International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, June 17-20, 2013, Bolton Landing, New York. Iowa City, IA: Public Policy Center, University of Iowa, 2013: 404-410. h=ps://doi.org/10.17077/drivingassessment.1519 http://hfast.mie.utoronto.ca/wp-content/uploads/Publications/CSRC_UofT_Report_Literature_review_and_driver_feedback_model.pdf

[4] Ibid.

[5] Ibid.

[6] Daniel Braun, Ehud Reiter, Advaith Siddharthan, Department of Computing Science, University of Aberdeen. Creating Textual Driver Feedback from Telemetric Data. In: Proceedings of the 15th European Workshop on Natural Language Generation (ENLG), pages 156–165, Brighton, September 2015. https://www.aclweb.org/anthology/W15-4726

[7] Feng, Jing and Donmez, Birsen. Design of Effective Feedback: Understanding Driver, Feedback, and their Interaction. In: Proceedings of the Seventh International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, June 17-20, 2013, Bolton Landing, New York. Iowa City, IA: Public Policy Center, University of Iowa, 2013: 404-410. h=ps://doi.org/10.17077/drivingassessment.1519 http://hfast.mie.utoronto.ca/wp-content/uploads/Publications/CSRC_UofT_Report_Literature_review_and_driver_feedback_model.pdf

Behavioural economics shows us that people will repeat behaviours that are rewarded[8]. Applying this principle to driver feedback, a driver would be expected to repeat behaviour that was indicated to them was successful. For example, a driver that can see, and is rewarded for, their improved merging technique onto the highway at a particular spot over time would naturally repeat that successful behaviour. This type of improvement would be drastically reduced without the use of geolocation data to provide effective positive reinforcement.

Effective feedback builds trust

Non-textual feedback elements, such as display of events on a map using geo-location data, allow a driver to visualize the trip information and provides justification for the feedback, which is crucial for a driver to trust and accept the textual feedback[9]. If drivers are unable to understand and reconstruct in the own minds how a score was calculated or a conclusion drawn, they will not trust the score.[10]

By offering the data on a map, drivers are given a chance to fully understand the feedback and make a very specific change that will have an outcome they can interpret. In other words, drivers are more likely to accept the feedback if they believe the information is being shared back to them in a meaningful way.[11]

Calibrate perception with performance

Drivers can miscalculate their own skill, and effective feedback can calibrate their perceived skill with their actual performance. They underestimate, for example, the impact that speeding, distracted driving or conversations with passengers have on their driving ability.[12] Young drivers in particular tend to overestimate their safety perimeters, which results in increased risk taking and a heightened confidence that leads them to underestimate the negative impacts that risky driving behaviour can have.[13] Plotting driving events through mapping allows drivers to recognize this mismatch in a positive and meaningful way, increasing their capacity to make positive change in their driving behaviour.

For example, a young driver may understand that using their cellphone while driving is dangerous and therefore they may choose not to do so when driving on major highways; however, they may still be prepared to take the risk when driving locally around town. If, upon reviewing their trip data on a map view, they can see that driving events happened while they were using their phone – when they believed they were in fact mitigating risk – this contextual feedback helps to highlight that their skills are not as good as they think they are. It reveals, for example, that it is risky to use a cellphone even when driving in urban areas. Without the visual context of plotting these events on a map for the driver to clearly see, the driver would only know that the events happened, and never understand that they actually happened when the driver believed they were being safe. Seeing the events overlaid on a trip map provides the recall assistance necessary for the driver to understand the events and choose to improve their driving behaviour.

---

[8] Center for Advanced Hindsight as cited at https://toolkit.bridgeable.com/behavioural-economics-principles

[9] Braun, D; Reiter, E; Siddharthan, A (2018). SaferDrive: an NLG-based Behaviour Change Support System for Drivers. Natural Language Engineering. 24(4): 551-588. http://oro.open.ac.uk/52968/1/saferdrive_accepted.pdf

[10] Daniel Braun, Ehud Reiter, Advaith Siddharthan, Department of Computing Science, University of Aberdeen. Creating Textual Driver Feedback from Telemetric Data. In: Proceedings of the 15th European Workshop on Natural Language Generation (ENLG), pages 156–165, Brighton, September 2015. https://www.aclweb.org/anthology/W15-4726

[11] Braun, D; Reiter, E; Siddharthan, A (2018). SaferDrive: an NLG-based Behaviour Change Support System for Drivers. Natural Language Engineering. 24(4): 551-588. http://oro.open.ac.uk/52968/1/saferdrive_accepted.pdf

[12] Donmez, B; Boyle, L; Lee, JD. (2008). “Mitigating driver distraction with retrospective and concurrent feedback” Accident Analysis and Prevention 40: 776–786 http://courses.washington.edu/cee500/Mitigating%20Driver%20Distraction%20with_Retrospective%20and%20Concurrent%20Feedback.pdf

[13] Behavior Change for Youth Drivers: Design and Development of a Smartphone-Based App (BackPocketDriver) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6334699/