

CSA GROUP™

STANDARDS RESEARCH

Rethinking Privacy Agreements

March 2020

Authors

Laura Fadrique, **M.Sc.,** University of Waterloo

Amethyst Kuang, University of Waterloo

Larissa Ugaya Mazza, University of Waterloo

Plinio Pelegrini Morita, **Ph.D., M.A.Sc., P.Eng.,** University of Waterloo

Advisory Panel

Victoria Hailey, The Victoria Hailey Group Corporation (VHG)

Jim Macfie, Microsoft Canada

Tania Donovska, M.Sc, CSA Group (Project Manager)

Stephen Michell, CSA Group

Jennifer Teague, **Ph.D.,** CSA Group

Table of Contents

Executive Summary 4

1. Introduction 5

2. Privacy Agreements 6

2.1 Laws and Acts in Canada 7

3. Challenges 8

4. Augmenting Privacy Agreements with Pictograms 9

4.1 Assessing Top Priorities 9

4.2 Exploring the Use of Pictograms for Privacy Agreements 11

4.2.1 Pictogram Design Process 12

4.3 Pictograms for Privacy Agreements 13

4.3.1 Overall Understanding of Privacy Agreements 15

4.3.2 Time Spent Reading Privacy Agreements 16

4.3.3 Frustration Experienced while Reading Privacy Agreements 17

5. New Layout Suggestion 18

6. Findings 19

7. Conclusions 23

References 24

Appendix A 29

Appendix B 30

Appendix C 31

Appendix D 32

Appendix E 33

Executive Summary

Technology is becoming an essential tool for supporting Canada's aging population and the use of technologies for this purpose is on the rise [1]. The deployment of products and services using new technologies often involves the collection of user personal data, and there are growing privacy concerns about how these data are collected and managed. Privacy agreements accompany products and services and are the primary source of privacy information for the users. All privacy agreements must comply with specific guidelines as presented by the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada [15]. Due to liability concerns, this often results in lengthy and complicated documents that are not user-friendly. As such, these agreements are often incomprehensible to the general public [13], [14].

The purpose of this research was to make current privacy agreements more transparent and easily comprehensible for the general public. This document describes the development and validation process of a new proposed privacy agreement layout that uses pictograms to represent the items in the agreement that matter most to users.

A survey was deployed to identify the top 10 concerns that users have with privacy agreements in Canada, the US, and Europe. The most significant concerns identified were:

1. *"The service would notify me in case of hacks or data leaks"* (Canada),
2. *"My data are deleted after I delete the app/account"* (US), and
3. *"If my data can be sold to third parties"* (Europe).

These concerns were modelled on the development of a privacy agreement layout using pictograms.

The pictograms were designed using the Double Diamond design method in an iterative design process. A graphical approach similar to the pictograms used for the identification of a workplace hazard was used [57]. A new layout for privacy agreements was assembled that included the pictograms representing the top 10 privacy concerns consolidated across all surveyed regions. A second survey was then deployed to evaluate the effectiveness of the newly developed pictograms in presenting information from privacy agreements.

The results showed that privacy agreements using pictograms improved readers' understanding of the content, reduced time spent reading the content and finding the information, and reduced frustration. Based on the findings above, augmenting current privacy agreements with pictograms is recommended for improving the accessibility and comprehension of long and complex documents.



"Users often buy new technologies and agree to privacy agreements without correctly understanding their contents."

1 Introduction

Market-bound, novel, health-related technologies are increasing on a daily basis [1]. The market for health care technologies, including the Internet of Things (IoT), is projected to reach USD$534.3 billion by 2025 [2]. Current projections suggest that IoT technology will reshape health care delivery models while also lowering health care costs [3]. This growth is best understood in the context of IoT technology's ubiquitous nature and extensive reach. IoT can be applied to a range of health care applications and purposes for people of all ages [4], including in the detection and monitoring of symptoms for physical and psychological conditions, as well as providing support to seniors in performing everyday activities in the community and especially at home [5]–[7]. Technology has become an essential component for supporting increased quality of life and aging at home for older adults and vulnerable individuals. It may be introduced in various forms, including access to online information [8], accessible communication with family and friends [8], and the use of new technologies such as Active Assisted Living (AAL) technology, smart homes, IoT, and wearables [6], [7].

With an ever-increasing presence in daily life, researchers and innovators predict that future users of health technologies will be more comfortable, familiar, and tech-savvy than earlier generations when integrating supportive solutions into their daily lives [9]. Despite the progress made so far, understanding technology, privacy, and security continues to be a challenge [10]. Users often buy new technologies and agree to privacy agreements without correctly understanding their contents and without knowing the full extent of what type of data are being collected or what services are being used [11].

Creating solutions to clearly communicate privacy agreements, and facilitate user comprehension, is the focus of this report. Due to the saturation of IoT and wearable technologies that collect personal and sensitive data 24 hours a day, in addition to other types of information (e.g., heart rate, blood pressure, body temperature) [6], the necessity for transparent and accessible information regarding privacy agreements is greater than ever. Each new device worn or used collects a distinct set of data and presents the user with a specific privacy agreement, indicating how the manufacturer handles their information. Generally, users are concerned with how their data are being collected and utilized by IoT and wearable technologies [12]. However, the length and complexity of these documents represent barriers to understanding [13], which usually results in users accepting privacy agreements without having a comprehensive understanding of the contents [11]. As a result of their challenges, these agreements usually fail to inform customers about how their data are treated because most users cannot understand the agreements and are dissuaded from reading them.

In addition to being complex, loaded with jargon, and challenging to read [13], [14], privacy agreements must also follow specific guidelines as presented by the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada [15]. Acts like PIPEDA in Canada and the General Data Protection Regulation (GDPR) in Europe [16] govern content rather than how information should be presented to users. Currently, it is at the discretion of each company to choose how to present the content of their agreements to users. Also, the level of transparency exercised to inform users of their practices concerning the collection and management of users' personal information is determined via each company's protocol [17].

This report aims to explore better ways of making existing privacy agreements more understandable and transparent through the use of a visual representation of their content. The goal is to propose a set of pictographic representations of critical information that could be presented at the beginning of privacy agreements, allowing easy, visual access to their content. To achieve the objective of creating the new pictographic layout, this study used surveys to identify the top 10 public privacy concerns related to data sharing and privacy agreements. Using the top concerns identified, a set of images was developed and validated through a second survey to determine the effectiveness of the new layout.

Ultimately, the proposed layout aims to improve the transparency of current privacy agreements and increase people's awareness of data collection by helping readers easily identify and understand them and their most important content.

2 Privacy Agreements

Privacy agreements, or privacy policies, are legal statements disclosing how an entity collects, uses, shares, and manages their users' data [18]. These agreements function as one of the primary principles for protecting people's privacy online through the provision of an informed agreement [19].

The role of privacy agreements is to help users better understand what data are being collected, how the collected data are used, and who can access the data [19]. By having data-collecting entities disclose the treatment of collected user data, people are provided with information that lets them decide if they want to interact with the entity or not [20]. Additionally, the agreements help data-collecting entities build user trust by addressing privacy concerns in these policies, which can reduce users' fear of sharing their data with the entity and increase their willingness to do so [19], [20].

Privacy agreements are commonly built around the principles of fair information practices [21]. The principles were first mentioned in 1973 in a report by the US Department of Health, Education, and Welfare, titled *Records, Computers, and the Rights of Citizens* [21]. They were created to allow the benefits of computerization to continue to advance in medical recordkeeping while providing safeguards for patient privacy [22]. Currently, the eight most cited fair information practice principles for privacy agreements come from the Organisation for Economic Co-operation and Development (OECD), which are:

1. Collection limitation;
2. Data quality;
3. Purpose specification;
4. Use limitation;
5. Security safeguards;
6. Openness;
7. Individual participation; and
8. Accountability [17].

Today, these principles are still widely adopted by various privacy policies, including the US Health Insurance Portability and Accountability Act (HIPAA), the European GDPR, and those created by the OECD, the Canadian Standards Association (CSA) [21], the US Federal Trade Commission, and the Asia-Pacific Economic Cooperation [23]. The wide adoption of these key privacy policies can be attributed to two key benefits.



"Privacy agreements, or privacy policies, are legal statements disclosing how an entity collects, uses, shares, and manages their users' data"

First, they have enough flexibility to serve as building blocks for new regulatory proposals [17]. Second, they enable the harmonization of data protection protocols by providing a common set of values, which is necessary for data to flow between different countries and to provide a benchmark for industries, advocates, and policymakers to analyze new technologies [17].

Although the eight, fair information practice principles of the OECD are reflected in the regulations of many countries, their implementation occurs differently across jurisdictions [24]. Privacy agreements created for international use, specifically for online use, are built around the Federal Trade Commission's five widely accepted fair information practice principles, which are:

1. Notice;
2. Choice;
3. Access;
4. Security; and
5. Enforcement [20].

These five principles were chosen after the Federal Trade Commission revised the US, Canada, and European fair information practice principles and concluded that the five topics were common to all documents and could be classified as the five basic principles of privacy protection [23].

2.1 Laws and Acts in Canada

Canada's Model Code for the Protection of Personal Information (1995), contributed to the basis for the principles of fair information practices used today in other privacy policies [21]. It was later enacted into PIPEDA in 2000 [21]. The Model Code currently presented by PIPEDA is composed of 10 principles, as presented in Figure 1 [15].

Figure 1: *The 10 privacy principles of PIPEDA*

1	Accountability
2	Identifying Purposes
3	Consent
4	Limiting Collection
5	Limiting Use, Disclosure, and Retention
6	Accuracy
7	Safeguards
8	Openness
9	Individual Access
10	Challenging Compliance

PIPEDA is longer and more detailed than any of the other policies currently available [21]. Due to its length, the implementation of PIPEDA is also noteworthy for its complexity [21]. Its broad scope ensures that the same rules apply to all organizations and encourages greater consistency across privacy policies [22], [25]. It ensures that people are provided with a standard that they can use to judge how their personal information is being treated and it helps increase their awareness of their privacy rights [22]. PIPEDA provides a common benchmark for measuring the adoption of data protection, allowing users to quickly identify which business practices are privacy-friendly, as well It also supports companies so that they do not need to "reinvent the wheel" when developing their privacy policies [25].

3 Challenges

A key issue with PIPEDA, which is common among privacy policies that are based on the principles of fair information practices, is that it was written before the rise of technologies such as social media platforms, connected personal device (smartphones, smartwatches, tablets) applications, and the ubiquitous tracking of said devices by the companies that provide the products. Current privacy agreement models are not well adapted to new technologies and practices, including the collection of "big data" via smart devices, since the principles they have been built around were designed to address relatively simple data processing problems [17].

The principles of fair information practices focus on data aggregation by industries and do not consider individuals' vulnerabilities on platforms such as social media, where they are susceptible to being manipulated by others and may struggle to make safe decisions due to the limited cognitive abilities of humans in general and/or practical resources [17]. For example, a person's decision to agree to a company's privacy practices can be affected by how a company presents and phrases its privacy agreements [14], [17]. Additionally, people often have limited time to properly read and understand the privacy agreements they are presented with, particularly given the plethora of new applications and connected devices adopted over time [14], [17]. They also have limited control over the policy practices offered to them [13]. For example, while the current design of the agreements focuses on presenting users with the choice to accept or refuse an entity's privacy policies, customers often have to choose to accept all included practices, otherwise, they will not have access to the service [26].

Privacy agreements also face design criticism. As mentioned in the introduction, one of the major challenges of privacy agreements is that they are difficult to comprehend. In some cases, they are specifically designed to limit a company's liability rather than to optimize user-friendliness and understanding [13]. As a result, they are drafted with a focus on precision and inclusiveness rather than on informing users about how their data will be used and treated [13], [23]. This leads to privacy agreements being long, dense, and filled with legal jargon [14], [27], making them too complex for the average reader to understand [13] and often dissuading them from reading the policies [27]. Since users rarely read, understand, or even view the content of privacy agreements, the documents often fail to represent informed consent to the collection and use of the data they have outlined [27].

This scenario is problematic, as privacy agreements are designed around consent and control, which puts the responsibility of making choices related to data collection on users who are ill-prepared to make and accept the consequences of their choices [17], [26]. Users often do not have comprehensive information about the consequences of disclosing their data, nor the mechanisms to ensure that their data are only used in ways that they accept [14]. Thus, the heavy focus on customer consent and control over data can overwhelm, confuse, and mislead them [17]. Ultimately, as presented in the "paradox of choice" [28], providing users with too much control can cause them to become bewildered and agreeable to anything [17]. This turns privacy agreements into formal exercises designed to simply obtain consent to access and collect customers' data, using the idea of control to force ill-equipped people to be responsible for protecting their data [17].

It is important to note that in Canada and the US, privacy practices that are deemed more relevant to the general public are insufficiently addressed in these policy statements, regardless of whether they were created using the model code, the Federal Trade Commission's version of the principles of fair information practices, or the OECD privacy guidelines [29]. In other words, these statements fail to address people's privacy concerns, which may lead to reduced consumer trust in companies and less likelihood of sharing data with them [29]. Such scenarios emphasize the importance of exploring new approaches that can better communicate and create more accessible channels for privacy information.

4 Augmenting Privacy Agreements with Pictograms

The number of apps and technologies released in the consumer market is growing, and consequently, there is an increase in the volume of data being collected as well as privacy agreements being made available to the general public. It is necessary to explore new solutions to better communicate privacy content that is critical to users. This project focuses on creating alternative ways to communicate privacy rules to users, starting by first understanding the top 10 privacy concerns from users in Canada, the US, and Europe; followed by the design and evaluation of a new privacy agreement layout that incorporates images and pictograms.

4.1 Assessing Top Priorities

A survey was deployed to identify content from privacy agreements that users consider most important. The results were used to determine which privacy information should be conveyed using pictograms. The survey was designed using Qualtrics (CoreXM, Provo, Utah) and Amazon Mechanical Turk (MTurk) as the recruitment tool. Qualtrics is a platform that allows organizations to collect and analyze data from consumer experiences [30]. It includes a simple drag-and-drop tool that has a variety of adjustable components for researchers to design their surveys. For example, components for multiple questions, ranking, and scoring are available. Qualtrics was used first to create the questionnaires and the informed consent form for the study included at the very beginning of each questionnaire. Participants had to choose to provide consent to begin the survey. A link to the survey was generated using Qualtrics and MTurk was used to distribute the survey link and recruit study participants.

MTurk is a crowdsourcing website where individuals and organizations can outsource work to a distributed workforce who can perform tasks virtually [31]. The platform allows researchers to specify different recruitment filters for each task, such as the qualifications of prospective participants, and it allows researchers to remotely recruit participants regardless of their location. In this study, the inclusion/exclusion criteria of potential participants included location (i.e., Canada, the US, or Europe) and age (i.e., 18 years or older). A description of the study and instructions for the survey were provided to qualified prospective participants along with the survey link.

Each participant was presented with demographic questions along with questions about overall privacy concerns such as *"Are you concerned about your privacy while you are using the Internet?"* and *"Do you know what your online privacy rights are?"* The last question presented participants with a list of 29 potential privacy concerns, which were based on existing literature and surveys about privacy concerns and trust [32]–[39]. The topics include *"My data can be shared with third parties," "How my data are stored,"* and *"The service would notify me in case of hacks or data leaks."* Participants were asked to select 10 items from the 29 presented that represented their most significant concerns related to privacy agreements. In sequence, participants were asked to rank the 10 items they had selected in order of importance. The resulting list identified the top 10 concerns regarding privacy agreements in a ranked format, which allowed each item to be weighted for analysis.

The survey was deployed to participants with MTurk accounts created in Canada, the United States, and European countries. All participants were aged 18 or older, since this is a requirement for becoming a worker on MTurk, and sorted into age groups of 18–25,

26–30, 31–35, 36–45, 46–55, and 56–99. The results were analyzed as a single group and stratified by the participants' home country and age.

A total of 391 participants answered the survey. To identify the top 10 concerns, the answers provided by the participants for the ranking portion of the survey were analyzed according to a weighted protocol in which items appearing in the first place received a score of 10; when they appeared in the last place, they received a score of 1. The results were aggregated and the topics were ranked based on the weighted scores, yielding the top 10 concerns in order of priority (Table 1).

While recruitment efforts for the questionnaires were equal across the three regions (Canada, the US, and Europe), participation was largest among the population of the US (Figure 2). This result matches the demographic representation of MTurk workers, which indicates that there are more workers in the US (75% in total) than in the other two regions [40].

Table 1: *Top 10 concerns related to privacy agreements. The scores presented in the table correspond to the total sum of all participants after applying a weighted score*

RANK	CONCERN	SCORE
1	If my data can be sold to third parties	1365
2	My data are encrypted	1323
3	My data are deleted after I delete the app/ account	1266
4	The purpose of collecting my data	1228
5	The data collected are anonymized	1956
6	It is possible to opt out from the service	1049
7	The service would notify me in case of hacks or data leaks	1024
8	It is possible for me to manage my own data (e.g. view, update, delete, or transfer)	957
9	Which data types are being collected (e.g. heart rate, steps, etc.)	930
10	My data are being collected	929

Figure 2: *Survey demographic results*

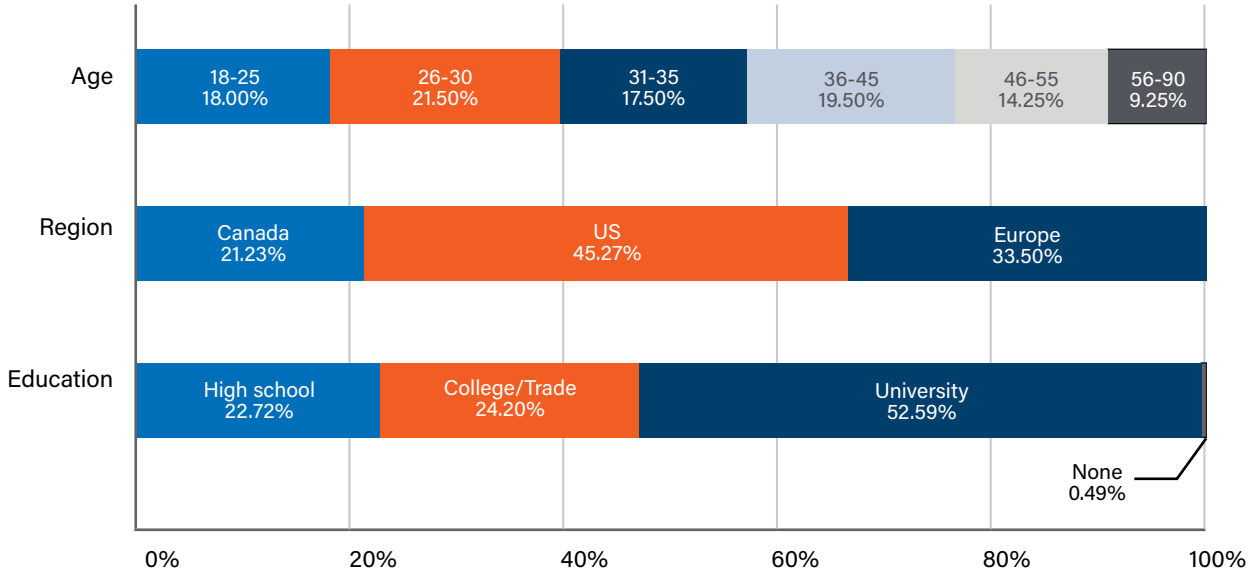


Figure 3 shows the list of top 10 concerns sorted by the overall score from largest to smallest and divided by region. The scores are adjusted for the number of participants per region. As can be seen, the order of the top 10 items differs according to the region. Canada's participants prioritized *"The service would notify me in case of hacks or data leaks".* Europeans ranked the item, *"My data are deleted after I delete the app/account,"* as the most significant concern. Meanwhile, the US ranked *"If my data can be sold to third parties"* as their top priority. This difference in ranking could be attributed to the regions having different cultural values and privacy regulations that shape each other, resulting in differing data privacy cultures that affect participants' perception of the privacy topics [41].

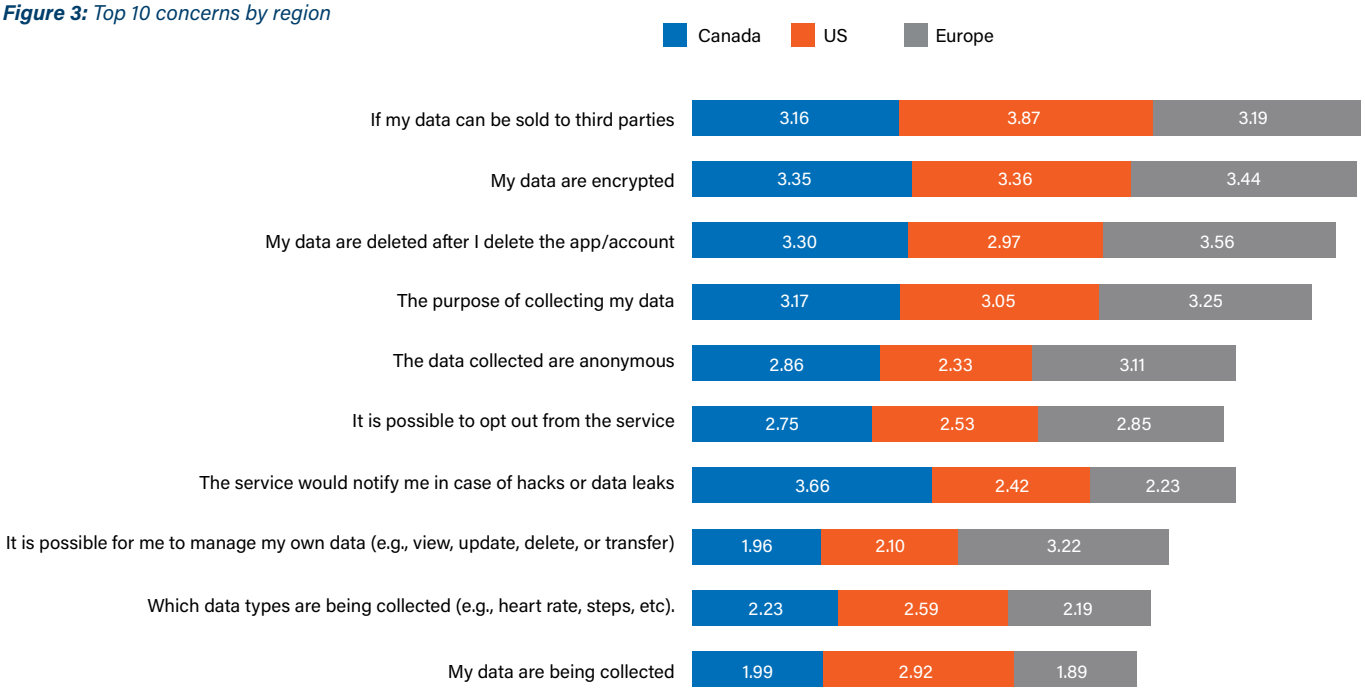
4.2 Exploring the Use of Pictograms for Privacy Agreements

A new layout was explored, taking into account the top 10 concerns related to privacy agreements that were identified from the survey. The development of this augmented representation of the agreements was derived from a literature review that focused on the creation of pictograms for the identification of hazards.

Pictograms can be beneficial when communicating information. They can warn the reader about possible dangers at a glance and be more easily understood than their written counterparts [42]. When using a pictogram, the advantages range from being more easily recognized and remembered in the future to attracting more attention and improving understanding for people with literacy or visual deficiencies [42]–[48]. Previous studies have shown that the inclusion of pictograms greatly benefit readers, who thought the images helped them identify, recognize, and be aware of the dangers a certain product posed [42], [48]–[56].

According to the Canadian Centre for Occupational Health and Safety (CCOHS), pictograms are defined as *"graphic images that immediately show the user of a hazardous product what type of hazard is present. With a quick glance, you can see, for example, that the product is flammable, or if it might be a health hazard."* They are generally comprised of two graphic parts and two textual parts. The graphic parts include the border (usually a red square set on one of its points) and the symbol (a black image inside of the red border). Combined, these two parts constitute a pictogram [57].

Figure 3: *Top 10 concerns by region*



A written section usually accompanies every pictogram, with a bolded text indicating the name of the pictogram, and a smaller text in brackets describing the hazard. Figure 4 shows examples of hazard pictograms.

Pictograms have ideal use cases. Images are more appropriate to represent material things, relative size, and simultaneous concepts, but they are not very good at representing general or abstract concepts [58], [59]. When dealing with generalization and abstraction, words are usually more informative [58].

4.2.1 Pictogram Design Process

Laughery and Wogalter [46], [60], and Emery *et al.* [44] reviewed the elements that a pictogram must have to be considered effective: the ability to attract attention, elicit knowledge and enhance comprehension, and the ability to enable compliance behaviour. These authors also present design factors and non-design factors that may hinder a pictogram's efficiency. Design factors are related to the design of the pictogram (e.g., format, colour, symbols, and connotation). Non-design factors have to do with the context separated from the design (e.g., familiarity, literacy, stress, and previous knowledge).

An important part in the making of pictograms is defining the process to create something more efficient. The guideline implemented for the creation of the pictograms presented in this report is:

- Co-developing the pictogram with users and developing the pictograms using an iterative method [43], [51], [61]–[65];
- Testing the pictogram with users [43], [47], [48], [52], [61], [63]–[65];
- Building the pictogram on top of already existing systems [58], [64];
- Implementing pictures with labels as keywords or short texts [45], [46], [51], [52], [64];
- Utilizing colour and contrast [46], [64], [66]; and
- Inserting the pictogram in the users' culture [45], [58], [61].

Employing a user-centred design methodology is considered by many as the most important aspect of pictogram development. This includes an iterative process that involves the users in the testing phase as well as in the design process. Such a process is necessary to enable designers to capture elements that

Figure 4: *Hazard pictograms (source: https://www.ccohs.ca/oshanswers/chemicals/whmis_ghs/pictograms.html)*

	**Exploding bomb** (for explosion or reactivity hazards)		**Flame** (for fire hazards)		**Flame over circle** (for oxidizing hazards)
	**Gas Cylinder** (for gasses under pressure)		**Corrosion** (for corrosive damage to metals as well as skin, eyes)		**Skull and Crossbones** (can cause death or toxicity with short exposure to small amounts)
	**Health Hazard** (may cause or suspected of causing serious health effects)		**Exclamation mark** (may cause less serious health effects or damage the ozone layer*)		**Environment*** (may cause damage to the aquatic environment)
	**Biohazardous Infectious Materials** (for organisms or toxins that can cause diseases in people or animals)				

**The GHS system also defines an Environmental hazards group. This group (and its classes) was not adopted in WHMIS 2015. However, you may see the environmental classes listed on labels and Safety Data Sheets (SDSs). Including information about environmental hazards is allowed by WHMIS 2015.*

might not have been initially considered by the designer or the specialists, resulting in pictograms that perform much better than the ones created without user input [43], [47], [48], [51], [52], [61]–[65].

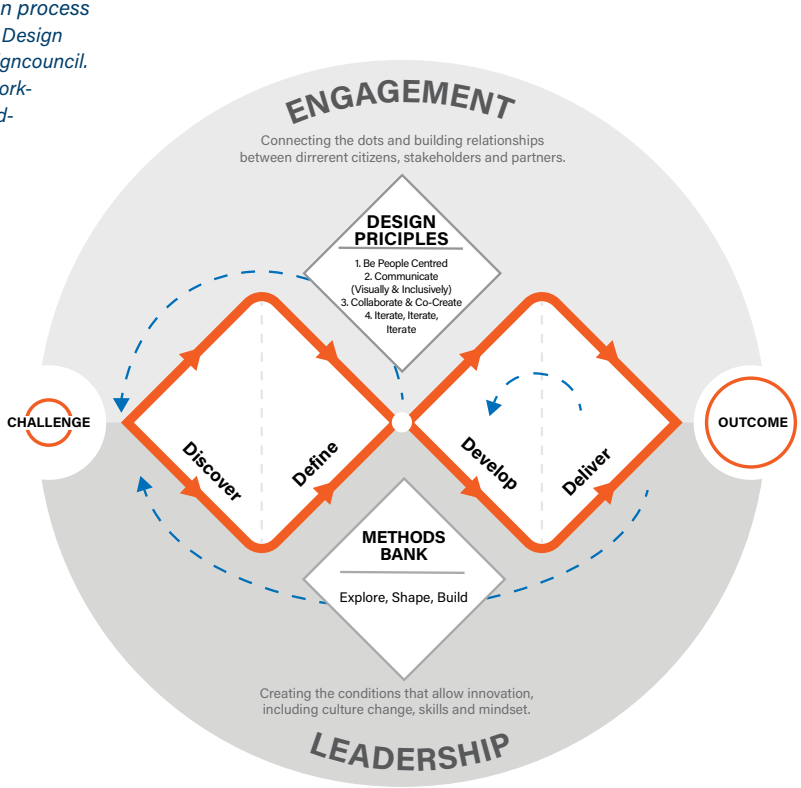
In the development of the pictograms, designers in this study practised a method called the Double Diamond design method (Figure 5), where iteration is a key part of the design process with multiple opportunities for interacting with users. The process begins in the **Discover** phase, where the theme is explored to better understand the user's needs, questions, and opinions on the problem. It is characterized by opening the scope of the research. This initial phase is followed by the **Define** phase, where the data that were collected previously are analyzed to identify patterns and themes, closing the scope. Next comes the **Develop** phase, in which tactics such as brainstorming, sketching, experiencing, and graphic recording are utilized in order to open the scope and develop the ideas found in the previous phases. The last is the **Deliver** phase, where solutions are prototyped based on previous developments and tested with users.

4.3 Pictograms for Privacy Agreements

Pictograms were developed using the Double Diamond design process to represent the ten greatest privacy concerns identified in the initial survey. A second questionnaire, created and distributed using Qualtrics and MTurk, was then deployed to evaluate the effectiveness of using pictograms to present information in privacy agreements.

Along with questions about participant demographics and their level of interest and concern regarding data privacy, this questionnaire compared the pictogram version of the agreements with the traditional version by presenting participants with the agreements in either their original format or the newly proposed pictographic format (Figure 6). The evaluation was performed using a between-subject design, where each participant was only exposed to one type of the document. Participants were asked to answer five questions about the treatment of their data based on the information presented in their agreement. This was followed by the participants rating their level of frustration when answering the

Figure 5: *Double Diamond design process (Reproduced with permission from Design Council). Source: https://www.designcouncil.org.uk/news-opinion/what-framework-innovation-design-councils-evolved-double-diamond*



© Design Council 2019

Figure 6: *Privacy agreement in standard (left) and pictographic (right) format, as presented in the questionnaire. Written privacy agreement source: https://www.fitbit.com/us/legal/privacy-policy.*

Privacy agreement

We believe that transparency is the key to any healthy relationship. At Fitbit, we're all about healthy. We appreciate that you are trusting us with information that is important to you, and we want to be transparent about how we use it.

Here we describe the privacy practices for our devices, applications, software, websites, APIs, products, and services (the "Services"). You will learn about the data we collect, how we use it, the controls we give you over your information, and the measures we take to keep it safe.

Specifically, we'll cover:

- Information We Collect
- How We Use Information
- How Information Is Shared
- Your Rights To Access and Control Your Personal Data
- Data Retention
- Analytics and Advertising Services Provided by Others
- Our Policies for Children
- Information Security
- Our International Operations and Data Transfers
- Changes to This Policy
- Who We Are and How To Contact Us

INFORMATION WE COLLECT

When you use our Services, we collect the following types of information.

INFORMATION YOU PROVIDE US

ACCOUNT INFORMATION
Some information is required to create an account on our Services, such as your name, email address, password, date of birth, gender, height, weight, and in some cases your mobile telephone number. This is the only information you have to provide to create an account with us. You may also choose to provide other types of information, such as a profile photo, biography, country information, and community username.

ADDITIONAL INFORMATION
To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, like your logs for food, weight, sleep, water, or female health tracking; an alarm; and messages on discussion boards or to your friends on the Services.

You may also connect with friends on the Services or invite friends who have not yet joined by providing their email addresses, accessing social networking accounts, or using the contact list on your mobile device. We do not store your contact list and delete it after it is used for adding contacts as friends.

If you contact us or participate in a survey, contest, or promotion, we collect the information you submit such as your name, contact information, and message.

PAYMENT AND CARD INFORMATION
Some Fitbit devices support payments and transactions with third parties. If you activate this feature, you must provide certain information for identification and verification, such as your name, credit, debit or other card number, card expiration date, and CVV code. This information is encrypted and sent to your card network, which upon approval sends back to your device a token, which is a set of random digits for engaging in transactions without exposing your card number. For your convenience, we store the last four digits of your card number and your card issuer's name and contact information. You can remove the token from your account using your account settings. We do not store your transaction history.

If you purchase Fitbit merchandise on our website, you provide your payment information, including your name, credit or debit card number, card expiration date, CVV code, and billing address. We do not store this payment information. We store your shipping address to fulfill your order. Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms.

LIVE COACHING SERVICES
Our live coaching services are a platform for you to communicate with a live health, fitness, or wellness coach ("Live Coaching Services"). Coaches may be provided by third parties, such as your employer or insurance company, or by our third-party coaching service providers. If you use our Live Coaching Services, we collect information about such use, including the plan, goals, and actions you record with your coach, your calendar events, communications with your coach, notes your coach records about you, and other information submitted by you or your coach.

INFORMATION WE RECEIVE FROM YOUR USE OF OUR SERVICES

DEVICE INFORMATION
Your device collects data to estimate a variety of metrics like the number of steps you take, your distance traveled, calories burned, weight, heart rate, sleep stages, active minutes, and location. The data collected varies depending on which device you use. Learn more about the features of our various devices and how you can use MobileTrack. When your device syncs with our applications or software, data recorded on your device is transferred from your device to our servers.

LOCATION INFORMATION
The Services include features that use precise location data, including GPS signals, device sensors, Wi-Fi access points, and cell tower IDs. We collect this type of data if you grant us access to your location. You can always remove our access using your Fitbit device or mobile device settings. We may also derive your approximate location from your IP address.

USAGE INFORMATION
When you access or use our Services, we receive certain usage data. This includes information about your interaction with the Services, for example, when you view or search content, install applications or software, create or log into your account, pair your device to your account, or open or interact with an application on your Fitbit device.

Privacy agreement



We believe that transparency is the key to any healthy relationship. At Fitbit, we're all about healthy. We appreciate that you are trusting us with information that is important to you, and we want to be transparent about how we use it.

Here we describe the privacy practices for our devices, applications, software, websites, APIs, products, and services (the "Services"). You will learn about the data we collect, how we use it, the controls we give you over your information, and the measures we take to keep it safe.

Specifically, we'll cover:

- Information We Collect
- How We Use Information
- How Information Is Shared
- Your Rights To Access and Control Your Personal Data
- Data Retention
- Analytics and Advertising Services Provided by Others
- Our Policies for Children
- Information Security
- Our International Operations and Data Transfers
- Changes to This Policy
- Who We Are and How To Contact Us

INFORMATION WE COLLECT

When you use our Services, we collect the following types of information.

INFORMATION YOU PROVIDE US

ACCOUNT INFORMATION
Some information is required to create an account on our Services, such as your name, email address, password, date of birth, gender, height, weight, and in some cases your mobile telephone number. This is the only information you have to provide to create an account with us. You may also choose to provide other types of information, such as a profile photo, biography, country information, and community username.

ADDITIONAL INFORMATION
To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, like your logs for food, weight, sleep, water, or female health tracking; an

questions. The effectiveness of the proposed layout was assessed based on the rate of correct answers to the five data treatment questions, the amount of time spent answering those questions, and the perceived frustration of participants.

The recruitment efforts led to a total of 61 complete evaluations performed on Qualtrics, with 32 receiving a traditional version of a privacy agreement and 29 receiving an augmented version with pictograms. The participant sample can be better described by the data presented in Figure 7.

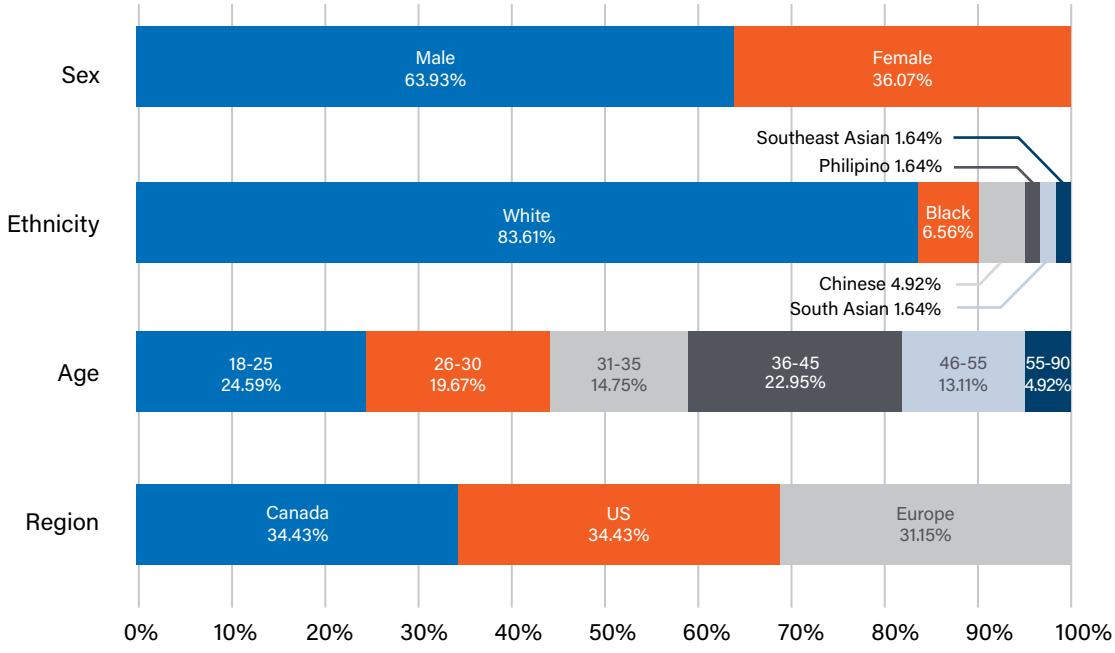
The participants had varying interests and concerns about privacy. A Pearson's correlation test was performed to assess the relationship between privacy concern levels and privacy knowledge levels. There was a statistically significant, moderate positive correlation between privacy concerns and privacy knowledge.[1] In other words, the more concern a participant felt about data privacy, the more they felt they knew about data privacy.

4.3.1 Overall Understanding of Privacy Agreements

The results of the analysis indicated a general improvement in efficacy by adding pictograms to the layout of the privacy agreement. Based on the participants' answers to the data treatment questions, participants' levels of understanding of the document increased by 14% with the pictograms (Figure 8 and Appendix A).

To investigate whether the differences in levels of understanding between the two layouts were significant, answers were consolidated by type: right, wrong, didn't want to read, didn't know answer. Fisher's exact tests were conducted for each answer type. The Fisher's exact test was selected since it is commonly used as an alternative for chi-square tests when there are categories with small sample sizes. In particular, the original layout had zero responses for the "Didn't want to read privacy agreement" category. In addition, the test can determine which answer types had a significant difference between the layouts.

Figure 7: *Results of the demographic questions used in the study*



[1] $r(98) = 0.34$, $p < 0.01$.

The results indicated that a participant's level of understanding was significantly associated with the layout that they were presented with[2] (see Appendix B). Answers stating that the participant "Didn't want to read the privacy agreement" and "Didn't know the answer" experienced insignificant changes between the different layouts. However, when pictograms were present, the frequency of correct answers significantly increased while decreasing significantly for incorrect answers, demonstrating that participants had a better understanding of the privacy agreement content.

4.3.2 Time Spent Reading Privacy Agreements

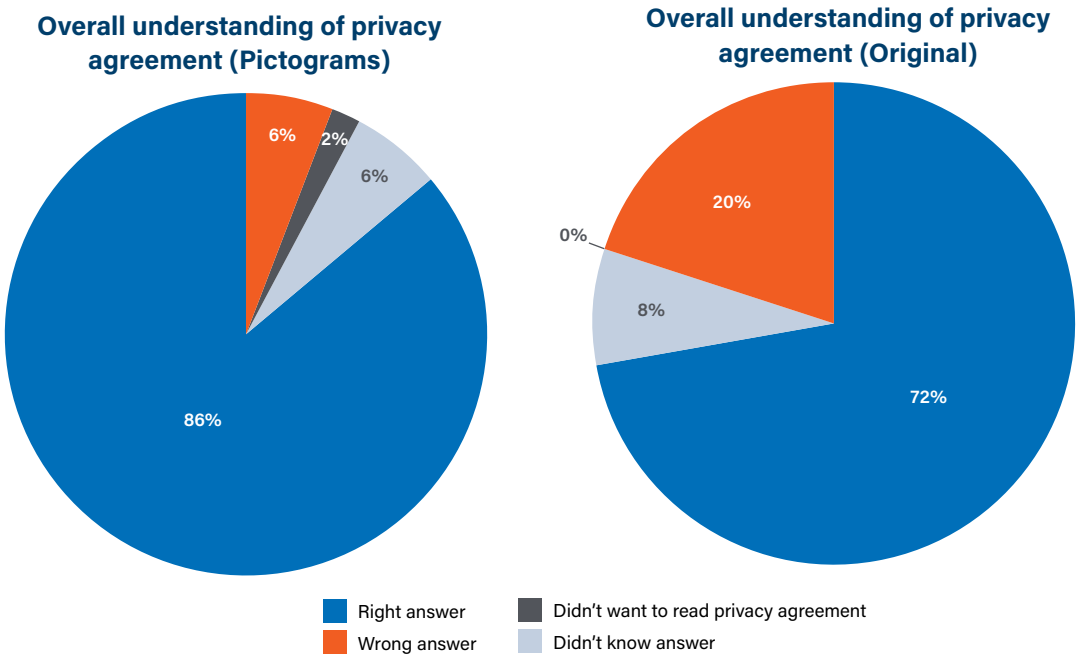
The quantity of time participants spent on each of the five questions decreased with the use of pictograms, as shown in Figure 9. All the questions, aside from the first, showed a decrease in the amount of time people took to find information and reach a conclusion.

To investigate if the decreases in time between the different layouts were significant, one-way Mann-Whitney U-tests were conducted for each question. The non-parametric *t*-test was selected because the distribution of data for each question was positively skewed and could not be transformed into normal distributions.

The tests found that only the decreases for questions 2 and 4 were significant[3,4] (see Appendix C). This could be due to different pictograms having differing levels of clarity. Nonetheless, with the addition of pictograms, the average total time participants took to finish answering all five questions decreased by 68.388 seconds. Therefore, it is possible that once the pictograms become universally used and commonplace, people will be more familiar with their meanings and be able to intuitively understand the information they represent, leading to a significantly decreased amount of time users spend on reading privacy agreements and finding information.

An alternative interpretation of the decrease in average total reading time could be that participants are only reading the summaries provided by the pictograms and not the original privacy agreements. This could be a concern as it suggests that people are not

Figure 8: *Comparison of overall understanding in the different layouts of privacy agreements*

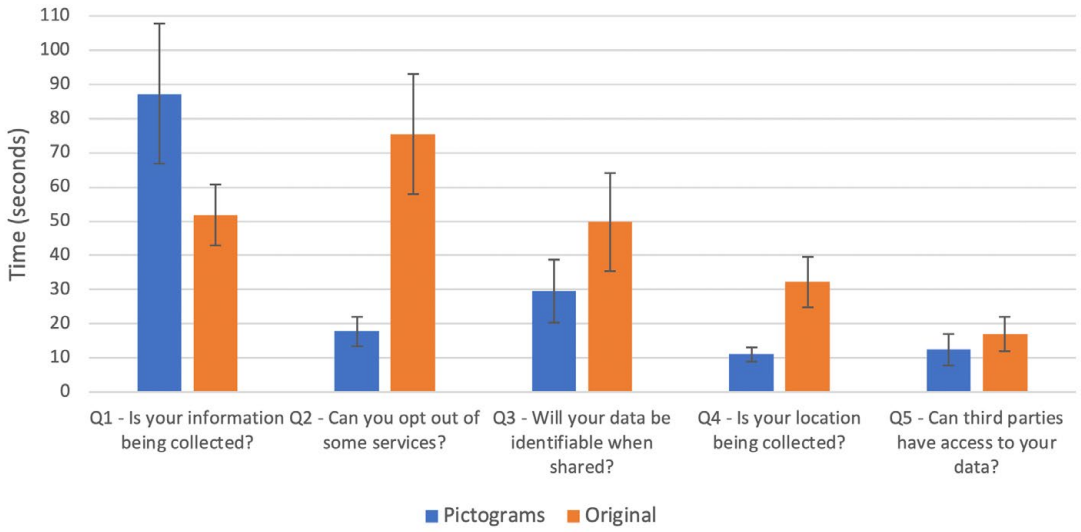


[2] Fisher's exact test *p*-value = 1.96e-04 **, α = 0.01.

[3] Question 2 *p*-value = 3.94e-05 **, α = 0.01.

[4] Question 4 *p*-value = 1.29e-03 **, α = 0.01.

Figure 9: *Average time (in seconds) spent on each question and standard error of each question*



reading and understanding the agreements they are accepting. However, when combined with the results for participants' overall understanding of privacy agreements, the results might also suggest that when presented with pictograms, participants still have a significantly better understanding of the privacy practices they are accepting even without reading the original document. In other words, users are not accepting the privacy agreements blindly.

4.3.3 Frustration Experienced while Reading Privacy Agreements

The perceived frustration of participants when answering the five questions decreased by 9% with the use of pictograms, as can be seen in Figure 10 (see also Appendix D).

To investigate if the differences in frustration levels between the privacy agreement layouts were significant, a chi-square test and a Fisher's exact test were conducted for each question. The chi-square test is a commonly used test to analyze the relationships between categorical variables. For this analysis, the privacy agreement layouts and the frustration levels were the focus. The Fisher's exact test was used as a post hoc test for the chi-square test to determine if there was a significant difference between frustration levels when participants engaged with the standard agreement layout versus the pictographic presentation.

The tests found that the overall frustration levels between the two layouts were not significantly different[5] (see Appendix E).

To investigate if participants' frustration levels when reading the agreements in the two layouts were affected by their data privacy concern levels, a Pearson's correlation test was conducted to assess the relationship between the level of frustration experienced and the level of data privacy concern participants exhibited. There was no statistically significant correlation between the level of perceived frustration and data privacy concerns for either layout[6,7].

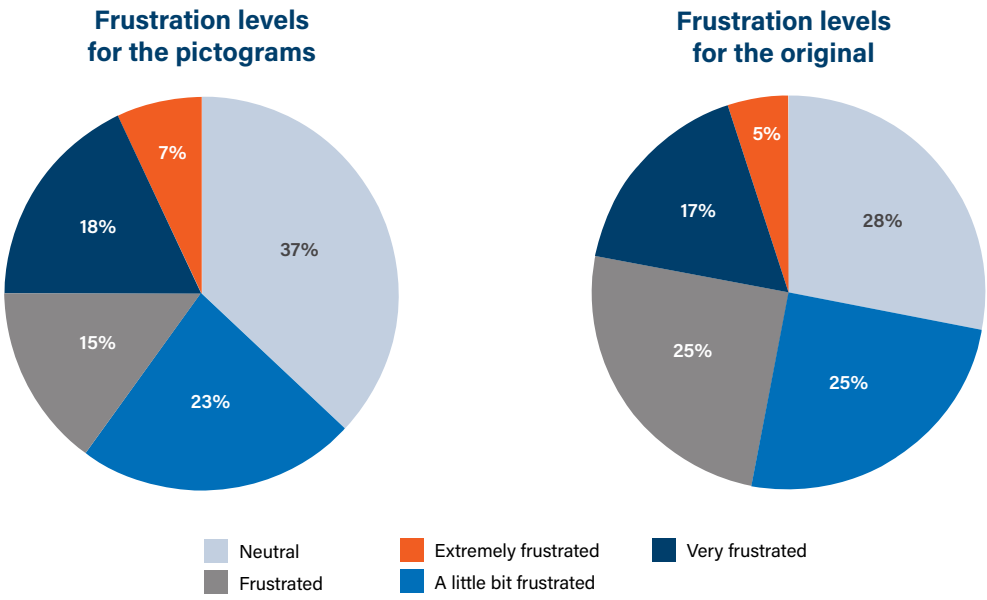
Overall, the results of this study show that pictograms might be a good solution for improving the comprehension of privacy agreements and their potential should be considered for wide-scale deployment.

[5] Chi-square test p-value = 0.45.

[6] Pictographic layout: $r(98) = -0.16$, $p = 0.42$.

[7] Original layout: $r(98) = 0.12$, $p = 0.50$.

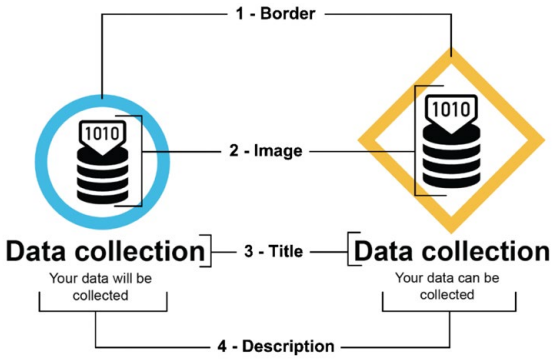
Figure 10: *Comparison of frustration levels in the different layouts of privacy agreements*



5 New Layout Suggestion

As has been described section 4.3, a new pictographic layout was proposed resulting from the design process. Each pictogram of the new layout has four different components, which are labelled in Figure 11.

Figure 11: *Pictogram anatomy*



The first component in Figure 11 is the border around each of the images, which are depicted either as a yellow diamond or a blue circle to differentiate between the warning and standard versions of the pictograms. Pictograms with the yellow border are designed to evoke the image of warnings to users, so they pay greater attention to these pictograms. Pictograms with the blue border are the standard pictograms. They are enclosed with a blue circle and are smaller to elicit less attention than the warning pictograms.

The second component is the black and white image inside each of the borders. Each image only uses thick lines and the colours black and white, following the same design principles used in the Material Design pictograms (https://material.io/resources/icons/?style=baseline). The black-and-white images of the pictograms are the same for the warning variation and the standard version, as seen in Figure 12.

The third component is the title under each image, written in bold right under the border. This is where the name of the pictogram is presented in no more than two words.

The fourth component is the short description of what the pictogram is meant to represent, and it is placed in a smaller font and regular case under the title. The proposed pictograms for some of the top 10 priorities identified can be found in Figure 12.

Figure 12: *Final pictograms (standard/blue and warning/yellow versions)*



Not all of the standard pictograms have a warning counterpart. This is because the warning pictograms solely represent the possibility of choice. However, some of the statements presented by the pictograms are simply notifications and are not choices to be made. For example, the standard pictogram for "you can opt out of some services" does not represent a choice and only informs the reader about what they can do. Thus, it has no warning pictogram to go with the message.

The new proposed layout for privacy agreements is shown in Figure 13. The first section, labelled 1, is reserved for pictograms representing data privacy features that the user can choose and control. It is marked by warning pictograms, so readers pay greater attention to these pictograms and the associated information. The second section, labelled 2, is for pictograms depicting features that cannot be changed. The third section, labelled 3, is for pictograms representing options that are given to the user, such as opting out of some services. The fourth section, labelled 4, is for the original privacy agreement as prepared by the company. The pictograms do not interfere with the agreement and only act as a summary.

Figure 14 depicts three possible applications for the privacy agreement layout in smartphone mode, with different pictograms in sections one, two, and three. The sections can increase in size or disappear completely, depending on the particular need of the document they are representing. Figure 15 depicts the same agreement with three possible applications formatted for the web.

6 Findings

The results of this study support the use of a pictographic layout as a guideline for companies trying to provide more transparency to their customers in their privacy agreements. The proposed layout shows promise in helping readers better understand how their data may be treated by data-collecting entities, which can be beneficial to both the users and the entities. Customers could benefit by becoming more informed, empowering them to evaluate an entity's privacy practices and have better control over their data. Meanwhile, companies and organizations could benefit from becoming more effective in addressing consumer privacy concerns

and building customer trust, which in turn would make customers more comfortable and more willing to share their data.

Pictograms provide an opportunity to help address several existing challenges within privacy agreements:

1. **Privacy agreements are too long and complex for readers to comprehend.** This challenge can be addressed using pictograms that summarize key privacy information at the beginning of the agreement. The pictograms could become standardized and be incorporated into a guideline regarding the content of privacy agreements. In turn, the guideline could be used as a benchmark for future services that evaluate the agreements to ensure they are easily accessible.

2. **Privacy agreement readers do not have the necessary resources to make the best decisions and understand the consequences of their decisions regarding their data**. Implementing a standardized set of pictograms as a guideline across various privacy policies will allow key information of privacy agreements to be summarized and presented in ways that are easy for users to make comparisons between different privacy practices. Subsequently, new services, such as training similar to WHMIS regarding pictograms, consequences, and control procedures [67], could also be created to inform and educate the general public on privacy topics.

Pictograms will require further improvement and development, followed by increased use to be easily understood. This could lead to future standardization, where companies and organizations could receive support in complying with privacy policies more easily while also meeting the accessibility needs of their customers.

Figure 13: *Proposed augmented privacy agreement, anatomy. Written privacy policy source: https://www.fitbit.com/us/legal/privacy-policy*

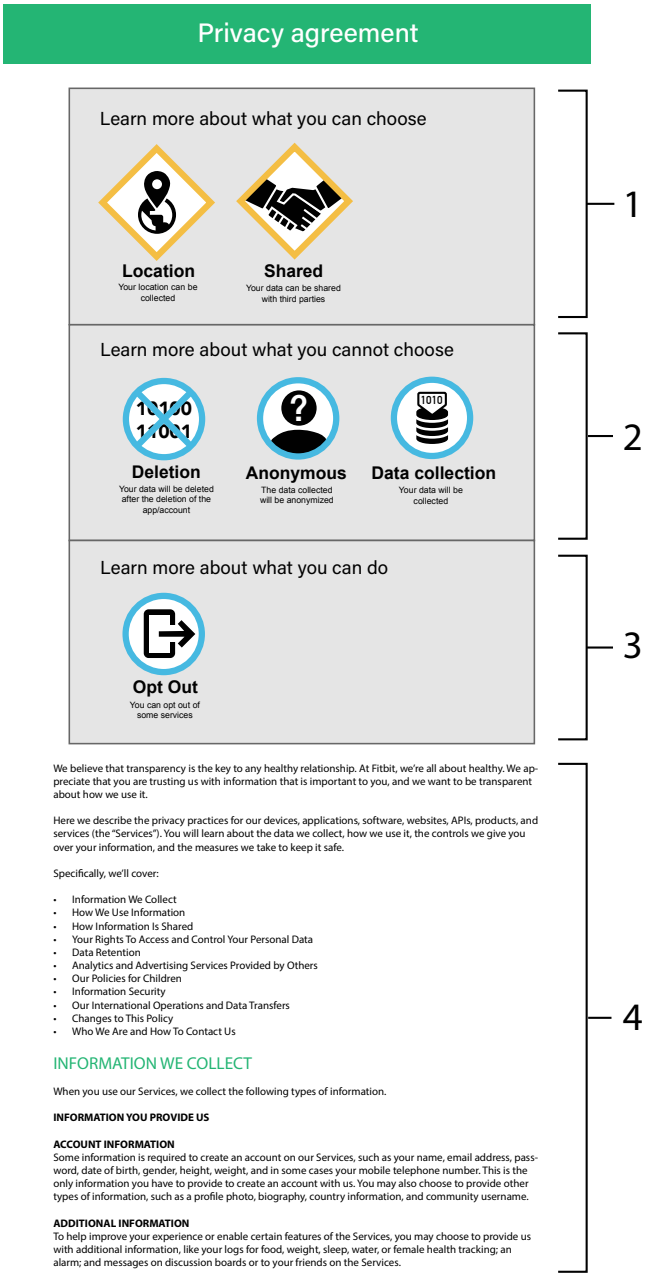


Figure 14: *Possible applications of the model (smartphone). Written privacy policy source: https://www.fitbit.com/us/legal/privacy-policy*

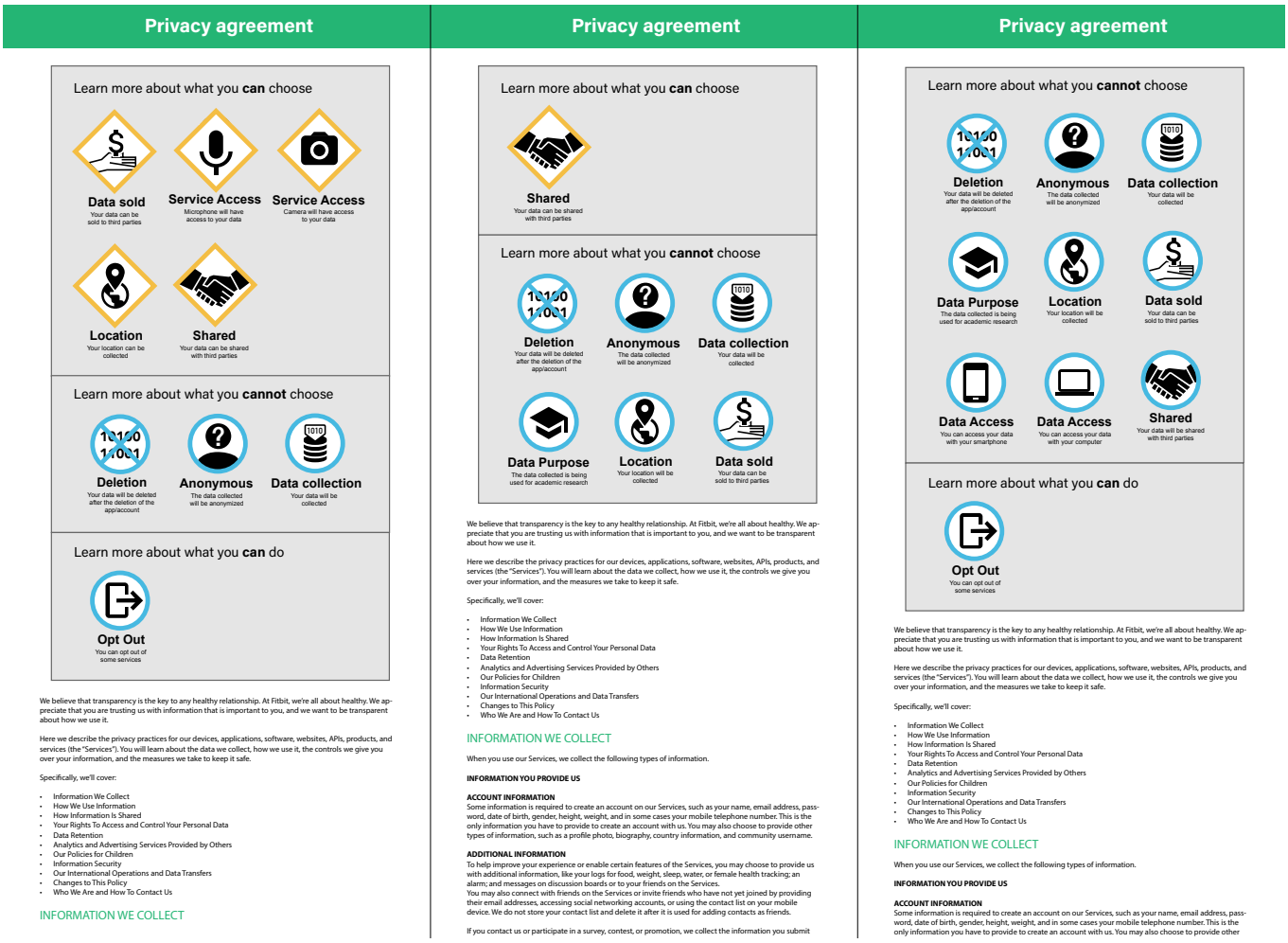
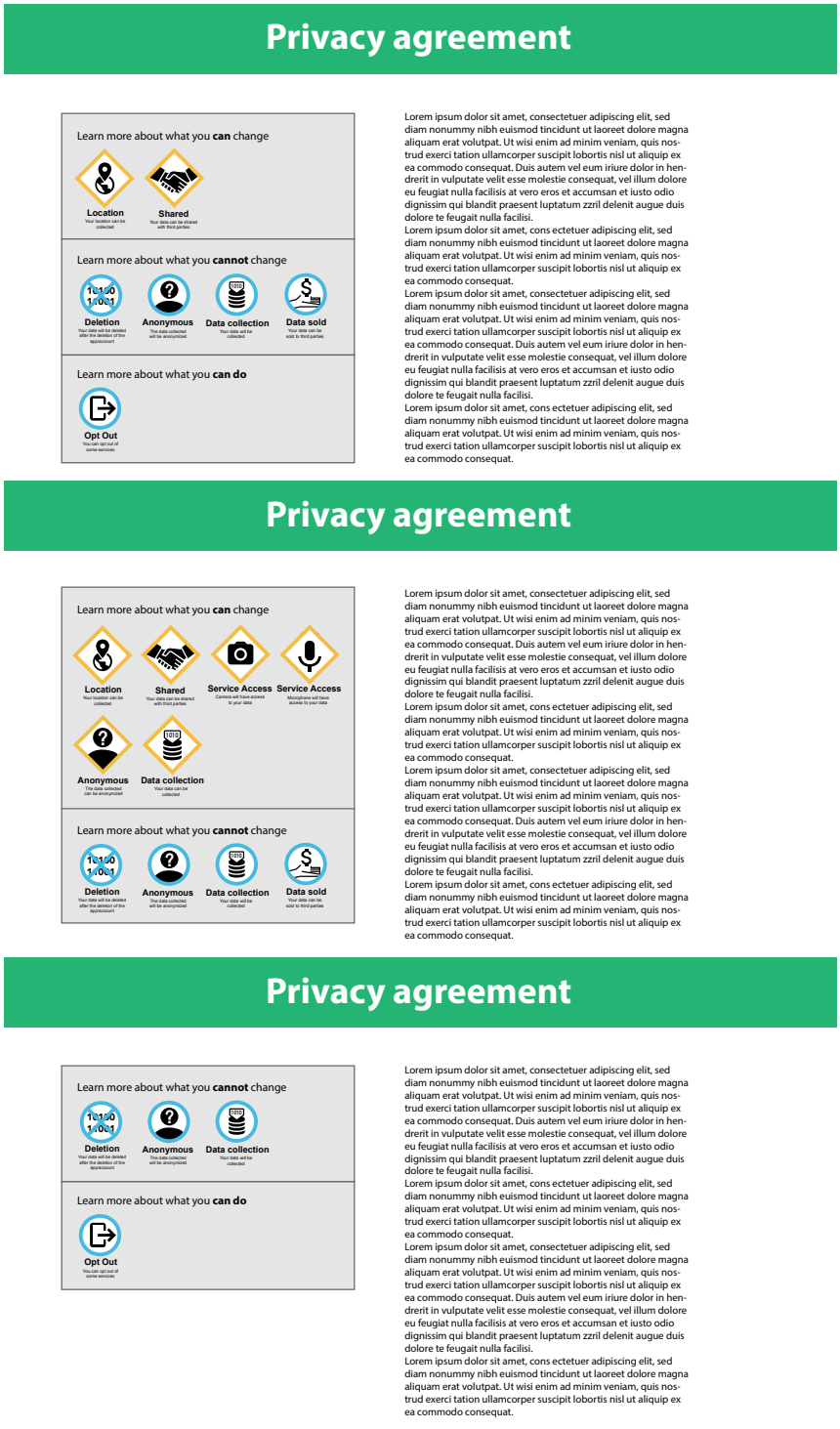


Figure 15: *Possible applications of the model (web). Written privacy policy source: https://www.fitbit.com/us/legal/privacy-policy*





The proposed layout shows promise in helping readers better understand how their data may be treated by data-collecting entities.

7 Conclusions

Data-driven technologies are becoming essential tools to support Canada's population with aging independently at home [6]–[8]. However, with the increasing use of these technologies, there are also growing privacy concerns [12]. While privacy agreements are the main source of information for users, they are often incomprehensible to the general public due to liability concerns and legal jargon. This results in underinformed customers whose privacy concerns are insufficiently addressed [14], [29]. Users' privacy concern levels and the perceived importance of privacy policies are positively associated with the perceived importance of information transparency [68].

This study proposed a new pictographic layout for current privacy agreements to improve their transparency. The study first identified the top 10 privacy concerns that people selected as most relevant to them, followed by design and validation phases that explored the efficacy of a new layout in communicating information to readers. The implementation of pictograms in the agreement layout demonstrated the potential to make them more effective in terms of increased readability by clearly delivering information to users about how a data-collecting entity would treat customers' data.

The implementation of the pictographic layout as a guideline would provide companies and organizations with a basis to improve the accessibility of their privacy agreements. Users could then more easily identify key information and make comparisons between different privacy practices, thereby making more appropriate decisions about their data. Subsequently, they may also feel more confident in sharing their data to improve their own experiences. For instance, in the health sector, improving data sharing could help support and improve health research, public health surveillance, and individual health outcomes.

Privacy agreements are the main channel for users to understand how a company or organization manages their data. As such, it is a priority that their accessibility is improved to better inform and enable readers to have more awareness and control over how their data are being used and shared.

Reference

[1] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016.

[2] Grand View Research, "Internet of Things (IoT) in Healthcare Market Size, Share & Trends Analysis Report By Component (Service, System & Software), By Connectivity Technology (Satellite, Cellular), By End Use (CRO, Hospital & Clinic), By Application, And Segment Forecasts," GVR, San Francisco, CA, USA, 2019.

[3] B. Negash et al., "Leveraging Fog Computing for Healthcare IoT," in *Fog Computing in the Internet of Things,* A. Rahmani, P. Liljeberg, J.-S. Preden, and A. Jantsch, Eds., Cham, Switzerland: Springer International Publishing, 2018, pp. 145–169.

[4] S. Banerjee, A. Bhattacharya, S. Sen, A. Bhattacharya, and S. Sen, "Healthcare IoT (H-IoT)," in *Machine Learning and IoT: A Biological Perspective,* S. Sen, L. Datta, and S. Mitra, Eds., Boca Raton, FL: CRC Press, Taylor & Francis Group, 2019, pp. 247–263.

[5] B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, "Mobile-health: A review of current state in 2015," *J. Biomed. Inform.,* vol. 56, pp. 265–272, Aug. 1, 2015.

[6] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access,* vol. 3, pp. 678–708, 2015.

[7] S. Koch, M. Marschollek, K. H. Wolf, M. Plischke, R. Haux, and S. Koch, "On health-enabling and ambient-assistive technologies: What has been achieved and where do we have to go?" *Methods Inf. Med.,* vol. 48, no. 1, pp. 29–37, 2009.

[8] C. Siegel and T. E. Dorner, "Information technologies for active and assisted living—Influences to the quality of life of an ageing society," *Int. J. Med. Inform.,* vol. 100, pp. 32–45, Apr. 2017.

[9] M. Van Volkom, J. C. Stapley, and V. Amaturo, "Revisiting the Digital Divide: Generational Differences in Technology Use in Everyday Life," *N. Am. J. Psychol.,* vol. 16, no. 3, pp. 557–574 2014.

[10] L. X. Fadrique, D. Rahman, and P. P. Morita, "The Active Assisted Living Landscape in Canada – Insights for Standards, Policies, and Governance," CSA Group, Toronto, ON, CAN, 2019.

[11] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services," *Inf. Commun. Soc.,* pp. 1–20, Jul. 2018.

[12] A. Marakhimov and J. Joo, "Consumer adaptation and infusion of wearable devices for healthcare," *Comput. Hum. Behav.,* vol. 76, pp. 135–148, Nov. 2017.

[13] Federal Trade Commission, "Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Preliminary FTC staff report," FTC, Mississauga, ON, CAN, Dec. 2010. [Online]. Available: http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

[14] J. R. Reidenberg, N. C. Russell, J. Alexander, S. Qasir, and T. B. Norton, "Privacy harms and the effectiveness of the notice and choice framework," I/S: *J. L. & Pol'y for Info. Soc'y.,* vol. 1, pp. 485–524, 2015.

[15] Office of the Privacy Commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)," 2018. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[16] European Commission, "EU data protection rules," Jul. 2019. [Online]. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en

[17] W. Hartzog, "The inadequate, invaluable fair information practices," *Md. L.* Rev., vol. 76, 2017.

[18] USLegal Inc., "Privacy policy law and legal definition." Accessed Sep. 25, 2019. [Online]. Available: https://definitions.uslegal.com/p/privacy-policy/

[19] K. Martin, "Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online," *J. Public Policy Mark.,* vol. 34, no. 2, pp. 210–227, Sep. 2015.

[20] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," *Comput. Hum. Behav.,* vol. 28, no. 3, pp. 889–897, May 2012.

[21] R. Gellman, "Fair information practices: A basic history – Version 2.19," Oct. 7, 2019. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

[22] Privacy Rights Clearinghouse, "A review of the fair information principles: The foundation of privacy public policy," Oct. 1, 1997. [Online]. Available: https://www.privacyrights.org/blog/review-fair-information-principles-foundation-privacy-public-policy

[23] F. H. Cate, "The failure of fair information practice principles," 2006. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

[24] S. Bellman, E. J. Johnson, S. J. Kobrin, J. H. Lauder, and G. L. Lohse, "International differences in information privacy concerns: A global survey of consumers," *Inf. Soc.,* vol. 20, pp. 313–324, 2004.

[25] National Telecommunications and Information Administration, "Chapter 4: Elements of a self-regulatory regime," in *Privacy and Self-Regulation in the Information Age,* NTIA, Washington, DC, USA, Jun. 12, 1997. [Online]. Available: https://www.ntia.doc.gov/page/chapter-4-elements-self-regulatory-regime#4D

[26] F. H. Cate, "The Limits of Notice and Choice," *IEEE Security & Privacy,* vol. 8, no. 2, Mar. – Apr. 2010, pp. 59–62.

[27] M. K. Ohlhausen, "Privacy challenges and opportunities: The role of the federal trade commission," *J. Public Policy Mark.,* vol. 33, no. 1, pp. 4–9, Apr. 2014.

[28] P. P. Morita and J. A. Cafazzo, "Challenges and paradoxes of human factors in health technology design," *JMIR J. Hum. Factors,* vol. 3, no. 1, pp. 1–7, 2015.

[29] E. Boritz and W. G. No, "A gap in perceived importance of privacy policies between individuals and companies," in *Proceedings Congr. 2009 – 2009 World Congr. Privacy, Secur., Trust and Manag. E-bus,* Aug. 25–27, 2009, pp. 181–192.

[30] "Qualtrics XM, The Experience Management Platform Software." Accessed Sep. 3, 2019. [Online]. Available: https://www.qualtrics.com/

[31] "Amazon Mechanical Turk." Accessed Sep. 3, 2019. [Online]. Available: https://www.mturk.com/

[32] J. Tsai, L. Cranor, A. Acquisti, and C. Fong, "What's it to you? A survey of online privacy concerns and risks," Net Institute Working Paper No. 06-29, Oct. 2006. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=941708

[33] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Proc. of the Thirteenth Americas Conf. on Info. Systems,* Keystone, CO, Aug. 9–12, 2007. [Online]. http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

[34] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and protection for use on the Internet," *J. Am. Soc. Inf. Sci. Technol.,* vol. 58, no. 2, pp. 157–165, Jan. 2007.

[35] Office of the Privacy Commissioner of Canada, "2016 Survey of Canadians on Privacy: Final Report," Dec. 2016. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

[36] Open Data Institute and YouGov, "Attitudes towards data sharing," 2017. [Online]. Available: https://docs.google.com/spreadsheets/d/1A_y1XioG2Y4gSy7wXE3kivE40ZiwXrpIbj-YujY_-CQ/edit#gid=471882920

[37] K. Carras, R. Farmaha, K. Ramesh, and A. Santasheva, "Priv: Privacy simplified." University of Waterloo, 2018. Unpublished.

[38] Akamai, "Akamai Research: Consumer attitudes toward data privacy survey, 2018," 2018. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf

[39] RSA, "RSA data privacy & security report." Accessed: Mar. 17, 2020. [Online]. Available: https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf

[40] D. Difallah, E. Filatova, and P. Ipeirotis, "Demographics and dynamics of mechanical Turk workers," in *Proceedings of WSDM 2018: The Eleventh ACM International Conference on Web Search and Data Mining,* Marina Del Rey, CA, USA, February 5–9, 2018, pp. 135–143. [Online]. Available: https://doi.org/10.1145/3159652.3159661

[41] J. Budak, E. Rajh, and V. Recher, "Citizens' privacy concerns: Does national culture matter?" in Surveillance, *Privacy and Security,* M. Friedewald, J. P. Burgess, J. Čas, and R. Bellanova, Eds., London, UK: Routledge, 2017, pp. 36–51.

[42] W. Phimarn, L. Ritthiya, R. Rungsoongnoen, W. Pattaradulpithuk, and K. Saramunee, "Development and evaluation of a pictogram for Thai patients with low literate skills," *Indian J. Pharm. Sci.,* vol. 89, no. 1, pp. 89–98, 2019.

[43] M. Berthenet, R. Vaillancourt, and A. Pouliot, "Evaluation, modification, and validation of pictograms depicting medication instructions in the elderly," *J. Health Commun.,* vol. 21, no. sup1, pp. 27–33, Mar. 2016.

[44] S. B. Emery et al., "A review of the use of pictograms for communicating pesticide hazards and safety instructions: Implications for EU policy," *Hum. Ecol. Risk Assess Int. J.,* vol. 21, no. 4, pp. 1062–1080, May 2015.

[45] A. Nicol and S. Tuomi, "Hazard sign comprehension among illiterate adults," *Stellenbosch Pap. Linguist.,* vol. 37, pp. 67–88, 2007.

[46] K. R. Laughery and M. S. Wogalter, "Designing effective warnings," *Rev. Hum. Factors Ergon.,* vol. 2, no. 1, pp. 241–271, 2006.

[47] M. S. Wogalter, *Handbook of Warnings*, Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2006.

[48] S. Davies, H. Haines, B. Norris, and J. R. Wilson, "Safety pictograms: Are they getting the message across?" *Appl. Ergon.,* vol. 29, no. 1, pp. 15–23, Feb. 1998.

[49] G. Mok, R. Vaillancourt, D. Irwin, A. Wong, R. Zemek, and W. Alqurashi, "Design and validation of pictograms in a pediatric anaphylaxis action plan," *Pediatr. Allergy Immunol.,* vol. 26, no. 3, pp. 223–233, May 2015.

[50] E. Boelhouwer, J. Davis, A. Franco-Watkins, N. Dorris, and C. Lungu, "Comprehension of hazard communication: Effects of pictograms on safety data sheets and labels," *J. Safety Res.,* vol. 46, pp. 145–155, Sep. 2013.

[51] N. Kheir, A. Awaisu, A. Radoui, A. El Badawi, L. Jean, and R. Dowse, "Development and evaluation of pictograms on medication labels for patients with limited literacy skills in a culturally diverse multiethnic population," *Res. Soc. Adm. Pharm.,* vol. 10, no. 5, pp. 720–730, Sep. 2014.

[52] A. Korenevsky et al., "How many words does a picture really tell? Cross-sectional descriptive study of pictogram evaluation by youth," *Can. J. Hosp. Pharm.,* vol. 66, no. 4, pp. 219–26, Jul. 2013.

[53] T. H. Clawson, J. Leafman, G. M. Nehrenz Sr, L. Sandra Kimmer, and M. Usn, "Using Pictograms for Communication," *Mill Med,* vol. 177, no. 3, pp. 291–295, Mar. 2012.

[54] G. C. Ta, M. Bin Mokhtar, H. A. Bin Mohd Mokhtar, A. Bin Ismail, and M. F. B. H. Abu Yazid, "Analysis of the comprehensibility of chemical hazard communication tools at the industrial workplace," *Ind. Health,* vol. 48, pp. 835–844, 2010.

[55] R. Dowse and M. Ehlers, "Medicine labels incorporating pictograms: Do they influence understanding and adherence?" *Patient Educ. Couns.,* vol. 58, no. 1, pp. 63–70, Jul. 2005.

[56] L. E. Mansoor and R. Dowse, "Effect of pictograms on readability of patient information materials," *Ann. Pharmacother.,* vol. 37, no. 7–8, pp. 1003–1009, Jul. 2003.

[57] "Canadian Centre for Occupational Health and Safety." Accessed Sep. 4, 2019. [Online]. Available: https://www.ccohs.ca/

[58] C. G. Spinillo, "Graphic and cultural aspects of pictograms: an information ergonomics viewpoint," *Work,* vol. 41, no. Supplement 1, pp. 3398-3403, 2012.

[59] S. Ainsworth, "How do animations influence learning?" in *Recent Innovations in Educational Technology That Facilitiate Student Learning,* D. H. Robinson and G. Schraw, Eds., Charlotte, NC: Information Age Publishing, 2008, pp. 37–67.

[60] K. R. Laughery and M. S. Wogalter, "A three-stage model summarizes product warning and environmental sign research," *Saf. Sci.,* vol. 61, Jan. 2014, pp. 3–10.

[61] M. M. van Beusekom, A. H. Kerkhoven, M. J. W. Bos, H.-J. Guchelaar, and J. M. van den Broek, "The extent and effects of patient involvement in pictogram design for written drug information: A short systematic review," *Drug Discov. Today,* vol. 23, no. 6, pp. 1312–1318, Jun. 2018.

[62] R. Vaillancourt, M. P. Zender, L. Coulon, and A. Pouliot, "Development of pictograms to enhance medication safety practices of health care workers and international preferences," *Can. J. Hosp. Pharm.,* vol. 71, no. 4, pp. 243–257, 2018.

[63] C. R. Leite da Silva, C. Spinillo, and M. Soares, "As contribuições da linguagem gráfica pictórica para o design de avisos e advertências em medicamentos Ergonomia e design", 2007.

[64] R. Dowse and M. S. Ehlers, "Pictograms in pharmacy," *Int. J. Pharm. Pract.,* vol. 6, no. 2, pp. 109–118, Jun. 1998.

[65] Y. Liu, S. Chiu, Y. Lin, and W.-K. Chiou, "Pictogram-based method of visualizing dietary intake," *Methods Inf. Med.,* vol. 53, no. 6, pp. 493–500, Jan. 2014.

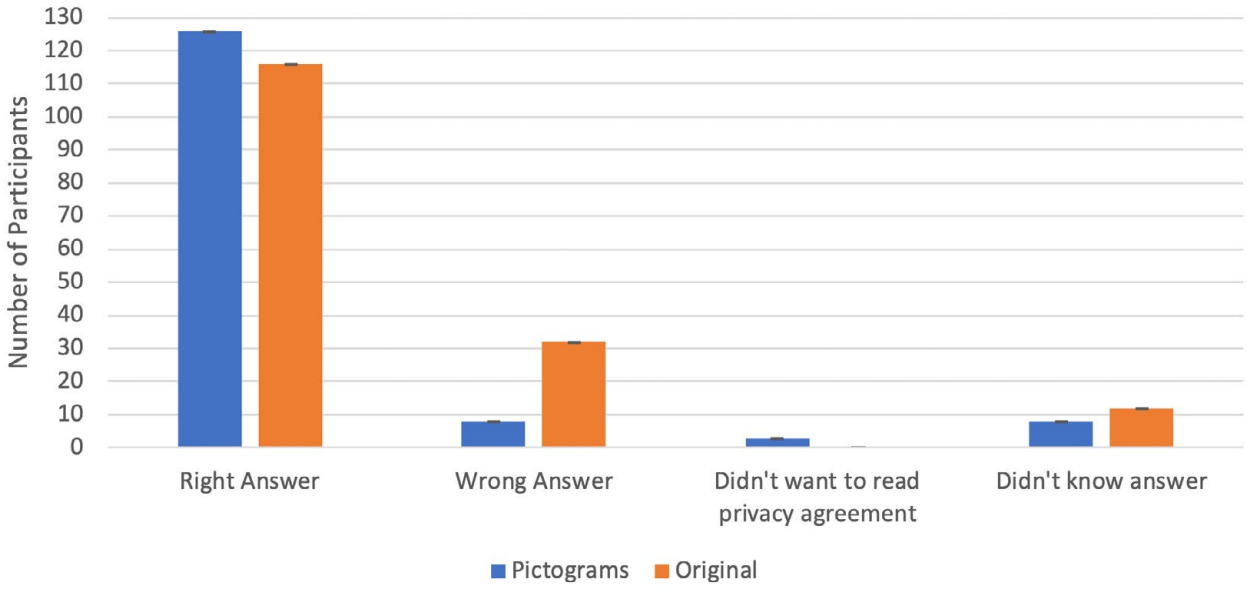
[66] J. F. Cavalcanti, M. M. Soares, and C. G. Spinillo, "Sinalização: um enfoque da ergonomia informacional e cultural," *Estud. em Des.,* vol. 17, no. 2, 2009.

[67] Canadian Centre for Occupational Health and Safety, "WHMIS.org | Canada's National WHMIS Portal." Accessed Oct. 22, 2019. [Online]. Available: http://whmis.org/

[68] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Q.,* vol. 30, no. 1, p. 13, 2006.

Appendix A

Number of participants per answer type and standard error of each answer type



Appendix B

Statistical values of comparing overall understanding between Pictograms and Original using Fisher's exact test (α = 0.01)

Fisher's exact test p-value		1.96e-04 **	
		Pictograms	Original
Right answer	Standard Error	0.03	0.03
	p-value	2.75e-03 **	
Wrong answer	Standard Error	0.01	0.02
	p-value	1.55e-04 **	
Didn't want to read privacy agreement	Standard Error	0.01	0.00
	p-value	0.11	
Didn't know answer	Standard Error	0.01	0.01
	p-value	0.50	

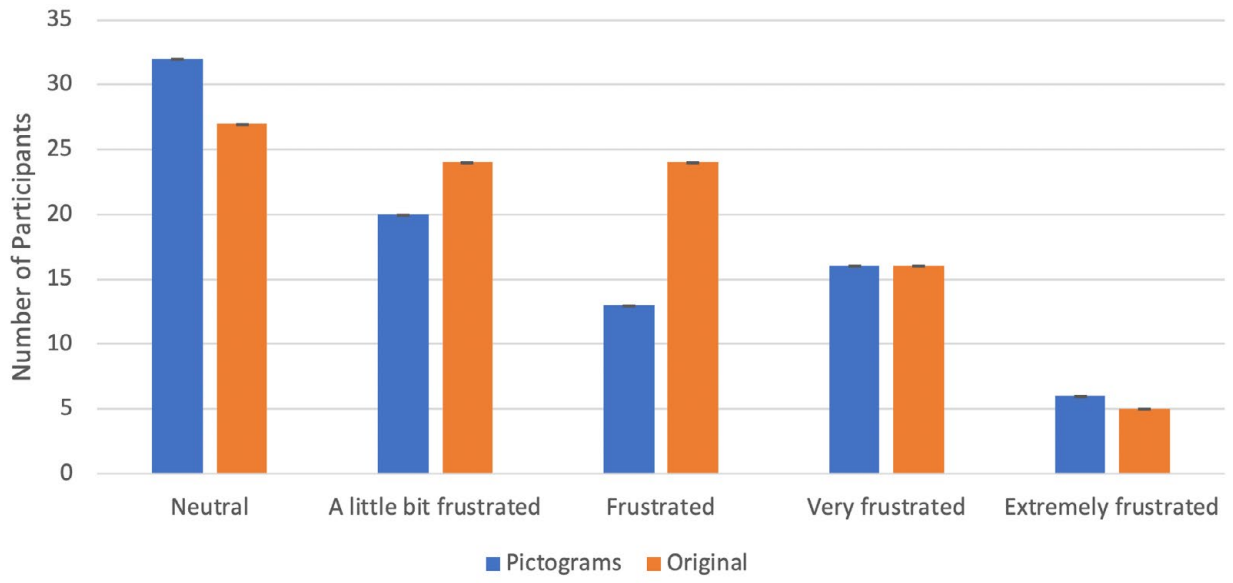
Appendix C

Statistical values of comparing changes in time (in seconds) for each question between Pictograms and Original using Mann-Whitney U-test (α = 0.01)

		Pictograms	Original
Q1	Median	50.62	37.50
	Average	87.28	51.85
	Standard Deviation	110.12	50.19
	Standard Error	20.45	8.87
	Wilcoxon Test Statistic	556.00	
	p-value	0.91	
Q2	Median	8.89	45.57
	Average	17.78	75.49
	Standard Deviation	22.78	99.47
	Standard Error	4.23	17.58
	Wilcoxon Test Statistic	199.00	
	p-value	3.94e-05 **	
Q3	Median	9.23	29.57
	Average	29.48	49.82
	Standard Deviation	49.38	80.75
	Standard Error	9.17	14.27
	Wilcoxon Test Statistic	388.00	
	p-value	0.14	
Q4	Median	7.74	18.16
	Average	11.08	32.26
	Standard Deviation	11.57	41.54
	Standard Error	2.15	7.34
	Wilcoxon Test Statistic	258.00	
	p-value	1.29e-03 **	
Q5	Median	6.03	5.58
	Average	12.48	17.07
	Standard Deviation	24.43	28.37
	Standard Error	4.54	5.01
	Wilcoxon Test Statistic	414.00	
	p-value	0.24	

Appendix D

Number of participants per frustration level and standard error of each frustration level



Appendix E

Statistical values of comparing frustration levels between Pictograms and Original using chi-square and Fisher's exact Test (α = 0.01)

CHI-SQUARE TEST	TEST STATISTIC	3.72	
	p-value	0.45	
		Pictograms	Original
Neutral	Standard Error	0.03	0.03
	p-value	0.27	
A little bit frustrated	Standard Error	0.02	0.02
	p-value	0.86	
Frustrated	Standard Error	0.02	0.02
	p-value	0.10	
Very frustrated	Standard Error	0.02	0.02
	p-value	0.85	
Extremely frustrated	Standard Error	0.01	0.01
	p-value	0.76	

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2020 Canadian Standards Association. All Rights Reserved.