Consumer Contracts, Copyright Licensing, and Control Over Data on the Internet of Things

Jeremy de Beer,[*] *Jules Belanger,*[**] *Mohit Sethi*[***]

Abstract

This article presents our interdisciplinary analysis of end-user license agreements and privacy policies from a sample of 22 consumer goods/services connected to the Internet of Things (IoT). We gathered data in the form of legal documents and assessed them from legal and economic perspectives. We developed an original taxonomy of IoT-connected consumer goods/services, classified different business models built around them, and reviewed legal terms and conditions related to their use.

Our analysis identifies copyright related restrictions and brings to light issues beyond copyright that merit consideration in the context of a review of copyright law and policy. First, we find that even obtaining legal information on smart products, including software license restrictions and other copyright limitations, is a difficult and time-consuming exercise. Second, our analysis of business models shows interoperability of platforms within an ecosystem of third-party devices and applications, but restrictions that limit interoperability across ecosystems. Third, terms and conditions of consumer use of smart devices in our sample are set up to allow for the collection and transfer of personal data, often sensitive data, in addition to all data collected by the companies from other sources such as social media. Fourth, our study shows that software licensing is now common practice among smart device manufacturers.

Based on these findings, we make recommendations to address the issues of accessibility of legal information, data portability, interoperability of systems, and competition. We recommend that governments cooperate with industry, consumer, and public interest groups to: (1) promote labelling standards to help consumers locate and understand the terms on which they acquire and use IoT products and services; (2) support open standards and protocols to facilitate interoperability across platforms; (3) integrate data portability and related issues with ongoing discussions about not only copyright reform but also reforms to privacy laws and other digital rights; and (4) take seriously the relevant recommendations of the Parliamentary Committee for revision to the *Copyright Act*.

---

[*] Professor at the Faculty of Law of the University of Ottawa.

[**] Economist at Option consommateurs.

[***] Student-at-Law at Borden, Ladner, Gervais LLP, Student Research Alumnus, Centre for Law, Technology and Society.

1. INTRODUCTION[1]

The year 2019 was a milestone year for Canada's *Copyright Act* as Parliament completed a mandated five-year statutory review.[2] In doing so, two Parliamentary committees tried to address numerous challenges posed by the so-called digital economy, such as ensuring fair compensation for creators while providing users with choice and quality content.[3]

Behind some of those challenges is the increasing connectivity of everyday objects, a major technological shift captured by the term, Internet of Things (IoT). The IoT generally refers to objects equipped with microcontrollers, sensors, and actuators, enabling the collection and the communication of a vast amount of data and creating a whole range of opportunities for data and analytics service providers. Facilitated by the use of smartphones and growing internet access and quality, the number of connected objects bought by Canadians has grown in recent years with applications ranging from security (wireless cameras, smart locks, etc.) to automation (smart lighting, smart thermostats, etc.) and health (smart thermometers, smart scales, etc.). The Canadian Internet Registration Authority (CIRA) estimates that one-third of Canadians are interested in acquiring a voice-controlled connected home device.[4]

Historically, purchasing consumer goods, even electronic ones, was governed by two areas of law: property and contract.[5] The good was the property and the purchase agreement was a contract. The rise of the IoT has sparked a number of issues related to copyright, competition, and other areas of law and policy. At the

---

1 The authors were commissioned by the Marketplace Framework Policy branch of Innovation, Science and Economic Development Canada (ISED) to perform the research underlying this article. This article is derived from a report presenting that research to the Government of Canada. This research was undertaken also thanks in part to funding from the Canada First Research Excellence Fund via the Plant Phenotyping and Imaging Research Centre, a digital agriculture research centre managed by the Global Institute for Food Security located at the University of Saskatchewan.

2 Every five years, the *Copyright Act* must be reviewed following the requirement introduced by the 2012 *Copyright Modernization Act*. The Standing Committee on Industry, Science, and Technology (INDU) filed its report on June 3rd, 2019. Although INDU had the official mandate to complete the statutory review, the Standing Committee on Canadian Heritage was asked to undertake a more limited assessment of remuneration models for artists and creative industries, which it released in a report on May 15th, 2019.

3 Government of Canada, *Parliament to undertake review of the Copyright* Act (14 December 2017), online: Government of Canada < https://www.canada.ca/en/innovation-science-economic-development/news/2017/12/parliament_to_undertakereviewofthecopyrightact.html > .

4 Canadian Internet Registration Authority, *2019 Canada's Internet Factbook* (April 2019), online: Canadian Internet Registration Authority < https://cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019 > .

5 Jason Schultz, "The Internet of Things We Don't Own?" (2016) 59:5 *Viewpoints* 36 at 36.

heart of the matter, software integrated to connected objects is redefining the notion of ownership of consumer goods.

In this new paradigm, consumers cannot conventionally "own" the goods they buy because software is merely licensed under conditions derived from copyright law protections.[6] Contractually, online transactions are conducted via clickwrap agreements.[7] Non-conspicuous terms of use and hyperlinks arguably do not provide buyers with adequate notice of the terms of agreement.[8] In fact, a study of end user license agreements, which used a list of the twenty-five most trafficked websites likely to have information on EULAs, found that buyers accessed these websites in only three out of 148,522 sessions.[9] As a result, consumers can unknowingly be limited in their ability to repair, modify, or sell the product.

This situation raises the question: in what circumstances would a limit on the freedom of contract be justified when contractual arrangements expand copyright protection?[10] Ian Kerr's prescient work on technological protection measures (TPMs) at the intersection of copyright and contracts[11] seeded related research by numerous scholars in Canada[12] and tracked thinking on this issue globally.[13] However, except for a very few statutory limitations that have been declared mandatory, there is still no definite guideline to determine whether limitations on copyright are imperative or not.[14] Related research on the legal rules governing tangible and intellectual property ownership addresses topics including, for example, the doctrine of exhaustion[15] and the division of

---

6 Aaron Perzanowski & Jason Schultz, *The End of Ownership: Person Property in the Digital Economy*" (Cambridge, MA: MIT Press, 2016) at Chapter 1.

7 Stacy-Ann Elvy, "Contracting the Age of the Internet of Things: Article 2 of the UCC and Beyond" (2016) 44 *Hofstra LR* 839 at 873.

8 *Ibid* at 875.

9 *Ibid* at 880.

10 Lucie MCR Guibault, *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* (Doctor of Laws, University of Amsterdam, 2002) at 197 [*Guibault*].

11 Ian R Kerr, Alana Maurushat, & Christan S Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill" (2005) 34:1 Ottawa L Rev 35, which was derived from a pair of studies commissioned by the Government of Canada.

12 See also Carys J Craig, "Digital Locks and the Fate of Fair Dealing in Canada: In Pursuit of 'Prescriptive Parallelism'" (2010) 13:4 *J World Intell Prop* 503; Pascale Chapdelaine, "The Ambiguous Nature of Copyright Users' Rights" (2013) 26 *Intell Prop J* 1.

13 See also Jacques de Werra, "Moving Beyond the Conflict Between Freedom of Contract and Copyright Policies: In Search of a New Global Policy for Online Information Licensing Transactions — A comparative Analysis Between US Law and European Law" (2003) 25:4 *Colum J L & Arts* 239; Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013); Radin, Margaret Jane, Access to Justice and Abuses of Contract, (2016) *Windsor Yearbook of Access to Justice*.

14 Guibault *supra* note 10 at 291.

constitutional powers.[16] Despite this vast body of literature, research that is based on empirical data, addresses the IoT, and/or is specific to Canada remains rare.

In practice, one widely reported example of recent controversy arose when farm equipment manufacturer John Deere tried to restrict farmers who tried to repair their tractors' software.[17] This, in turn, led some jurisdictions to introduce "right to repair" legislation[18] and helped grow a whole movement that is gaining traction in Canada.[19] In Québec, prior to tabling Bill 197 to *Amend the Consumer Protection Act to fight planned obsolescence and assert the right to repair goods*, a petition with 45,000 signatures was tabled in the National Assembly.[20] At the time of publication of this article, the Québec Bill remains in the public consultation phase. A similar Bill in Ontario was introduced in 2019 but failed to pass.[21]

New technological and commercial realities pose challenges to traditional copyright principles that policymakers have had a hard time dealing with. One key question is whether these issues should be federally governed or, like in the

---

[15] Shubha Ghosh & Irene Calboli, *Exhausting Intellectual Property Rights: A Comparative Law and Policy Analysis* (Cambridge: Cambridge University Press, 2018); Beer, Jeremy de & Robert Tomkowicz. "Exhaustion in Canadian Intellectual Property Law" (2009) 25 Canadian Intellectual Property Review 3—31.

[16] Jeremy de Beer, "Constitutional Jurisdiction Over Paracopyright Laws" in Michael Geist, ed, *In the Public Interest: The Future of Copyright Law Canada* (Toronto: Irwin Law, 2005) 89.

[17] Olivia Solon, "A right to repair: why Nebraska farmers are taking on John Deere and Apple" *The Guardian* (6 March 2017), online: <https://www.theguardian.com/environment/2017/mar/06/nebraska-farmers-right-to-repair-john-deere-apple>; "Why can't I fix my tractor?" (28 October 2015) (radio), online: CBC Radio <https://www.cbc.ca/radio/spark/297-the-future-of-food-farming-and-more-1.3275728/why-can-t-i-fix-my-tractor-1.3284537>.

[18] See the Massachusetts Right to Repair Initiative. See also: Emily Matchar, *The Fight for the "Right to Repair"* (12 July 2016), online: Smithsonian Magazine <https://www.smithsonianmag.com/innovation/fight-right-repair-180959764/>; Lean Chan Grinvald & Ofer Tur-Sinai, "Intellectual Property Law and the Right to Repair" (2019) 88:1 Fordham L Rev 63.

[19] See also the recent OpenMedia initiative: Lisa Xing, "Why a non-profit is pressing for 'right to repair' legislation in Canada" *CBC News* (2019 May 22), online: <https://www.cbc.ca/news/canada/toronto/right-to-repair-legislation-device-smartphone-1.5144235>.

[20] Bill 197, *An Act to amend the Consumer Protection Act to fight planned obsolescence and assert the right to repair goods*, 1st Sess, 42nd Leg, Québec, 2019 (Introduced on 9 April 2019); *Services Québec*, "Bill 197 against planned obsolescence and the right to repair — M.N.A. Guy Ouellette presents innovative bill to control planned obsolescence and the right to compensation" *Gouvernement du Québec* (10 April 2019), online: <http://www.fil-information.gouv.qc.ca/Pages/Article.aspx?lang=en&idArticle=2704109148>.

[21] Bill 72, An Act to amend the Consumer Protection Act, 2002 respect the repair of electronic products, 1st Sess, 42nd Leg, Ontario, 2019 (first reading 21 February 2019).

case of Québec, provinces should have their own legislation. A closely tied issue concerns portability of personal data and the interoperability of IoT platforms. For example, do consumers have a right to access the data collected and transmitted while using the connected object? Can this data be transferred from one company's ecosystem of apps to another? Is the license model adopted by companies impacting how long consumers can use their product?

To help respond to the Parliamentary review of the *Copyright Act* and better understand the challenges posed by the IoT to copyright law, we conducted empirical research on IoT-connected objects sold to Canadian consumers. The objective of our study was to perform an interdisciplinary analysis of end-user license agreements and privacy policies from a sample of consumer goods/services connected to the IoT. Therefore, we gathered data in the form of legal documents and assessed them from legal and economic perspectives. We developed an original taxonomy of IoT-connected consumer goods/service, classified different business models built around them, and reviewed legal terms and conditions related to their use.

Our article is divided as follows. We first present the methods we adopted for the research. We then discuss the main findings of our analysis based on the answers compiled from case studies. We finally summarize our findings and highlight what we think are key issues at stake for copyright law and the IoT.

2. METHODOLOGY

(a) Sampling Method

Our research was designed to "establish a sample of objects which constitute interesting cases and are part of the main categories of IoT consumer products (automobiles, home appliances, thermostats, watches, televisions, etc.)".[22] The first step was to consider the appropriate sampling method to use when selecting our list of connected objects.

It was not necessary to consider a full range of possible sampling methodologies. We decided that the sampling should be purposive, i.e. cases are chosen not at random but for a specific purpose. Purposive sampling requires screening and selection based on a number of pre-selected criteria. The criteria chosen depends on the precise research question to be answered.

The most promising potential sampling methods to choose from were the following:

- *Typical cases*: While not intended to be generalizable, typical case sampling does allow researchers to illustrate and compare different situations that appear similar.

---

[22] Quote is translated from the French-language mandate from ISED to conduct the research underpinning this article.

- *Deviant cases*: Deviant case sampling is the opposite of typical case sampling. Cases are selected because they are believed to be different to varying degrees, than the norm.
- *Critical cases*: If there are known examples of cases that are important to the study for one or more reasons, critical case sampling may be appropriate.
- *Heterogeneous cases:* The purpose of heterogenous sampling is to get maximum variation in the range of cases selected, providing the widest range of angles for analysis.
- *Homogeneous cases*: Homogenous case sampling is the opposite of heterogeneous case sampling. The goal is to limit variability, for example, to simplify or enhance comparability.

We opted to use each of these methods in appropriate circumstances. Where we were aware of particularly prominent products, such as the Apple Watch for example, we included them as critical cases. We were also aware of unique products, such as Amazon's AWS IoT Button, and included it as a deviant case. We suspected that within certain categories, like personal digital assistants, the products (although perhaps not their terms and conditions of use) would be relatively homogenous. In other categories, like home appliances, the products (although perhaps not their terms and conditions of use) would be relatively heterogeneous.

Following that, we determined whether the principal categories were the most interesting cases to study. If not, we needed to add to or refine these categories. Within each category, we determined the selection criteria on which to choose a sampling method and how many products to research. We discuss both steps in the following sections.

i) Sample Categories

The categories of IoT-related consumer goods identified were: automobiles, home appliances, thermostats, watches, and televisions. Preliminary research across a range of companies involved with IoT, such as IBM[23] and Intel[24] as well as advertising organizations[25] and consumer organizations,[26] showed there are many other ways to group goods into relevant categories.

---

[23] Jen Clark, *IOT use cases: the Internet of Things in action* (2016 October 25), online: International Business Machines - Internet of Things blog <https://www.ibm.com/blogs/internet-of-things/iot-use-cases/>.

[24] Intel, *A Guide to the Internet of Things* (Accessed on: 25 February 2019), online: Intel <https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png>.

[25] Interactive Advertising Bureau, *Nearly Two-Thirds of Americans Own at Least One Internet of Things Connected Device, With 65% Reporting They Are Willing to Receive Ads on IoT Screens* (2016 December 15), online: Interactive Advertising Bureau <https://www.iab.com/news/nearly-two-thirds-amerians-least-one-internet-things-connected-device/>.

After analyzing alternative classification schemes, we decided on the five consumer categories below:

1. **Connected cars**: Today's automobiles are moving data sensors and computers that capture information about the vehicle and access it in near real time.
2. **Wearables**: While health and fitness trackers are consumers' first step into the future, this category is quickly expanding into other devices like smart glasses and virtual reality tools.
3. **Home systems**: Smart homes require smart systems. IoT connected consumer goods that are *part of* the home, not just *in* the home, including thermostats, locks, and light bulbs.
4. **Home appliances**: The IoT is also entering homes through the appliances that consumers use every day, such as televisions, washing machines, refrigerators, and vacuum cleaners.
5. **Personal assistants**: Personal assistants like those from Amazon, Apple, and Google are used inside and outside the home, connected to speakers, smartphones, or other devices.

Devices with digital personal assistants were not mentioned as a category. But there is clear value in studying these devices, as they are the tools with which many other IoT devices are or soon will be powered. They also enable the study of intersecting technologies, like artificial intelligence. Digital personal assistants are often used in or with automobiles, but there were good reasons to maintain a distinction. For example, the type of data collected by digital personal assistants is likely much different than the data collected by connected cars. Moreover, studying connected cars on their own allows some separate consideration of the impact of copyright on consumers as self-driving cars become more ubiquitous. Connected cars also raise very different issues regarding the right-to-repair, and indeed may be the category of consumer-related IoT products where right-to-repair issues will be most widespread.

It also made sense to distinguish between home systems and home appliances. One is more permanent than the other (reflected in the legal distinction, at least at common law, between fixtures and chattels). There is also a more robust resale market for home appliances, on platforms like Kijiji for example, that raises distinct legal and technical issues. And while both home systems and home appliances could trigger right-to-repair issues, like connected cars, they do so in different ways. For connected cars, consumers would most typically work with an expert mechanic, whereas a do-it-yourself approach could be more common with home systems and home appliances. If third parties are involved, servicing of home systems would take place in the home.

---

[26] Option Consommateurs, *The Internet of Things Issues and Tips* (Accessed on: 10 July 2019), online: Option Consommateurs < https://option-consommateurs.org/the-internet-of-things/?lang = en > .

On the other hand, it makes sense to integrate specific kinds of appliances like televisions into a broader category of home appliances. Wearables, however, are sufficiently different from both home systems and home appliances to warrant a category on their own. The key difference is that consumers' wearables go with them inside and outside of the home.

ii) Sample Connected Products

Based on the five consumer goods categories identified above, we selected a number of specific products within each category. This selection reflects both homogeneous and heterogeneous case sampling, i.e. different sampling methods in different categories. An additional connected object was subsequently added to our initial sample based on our research findings. The full sample of 22 connected products is presented in the table below.

Table 2.1 — Sample of connected products

Categories	Products	Manufacturers
Connected cars	Autopilot ConnectedDrive NissanConnect Uconnect	Tesla BMW Nissan FCA
Wearables	Charge 3 Watch Series 4 Galaxy Watch Focals Go	Fitbit Apple Samsung North Oculus
Home systems	Learning Thermostat Hue Bulb Smart Lock Pro Pro 2	Nest Philips August Home Arlo
Home appliances	Roomba i7 + Family Hub SmarThingQ Laundry machine Bravia TV	iRobot Samsung LG Electronic Sony
Digital assistants	Home (Assistant) Echo (Alexa) HomePod (Siri) Bixby	Google Amazon Apple Samsung
Other	AWS IoT Button	Amazon

As the creator of one of the trendiest high-tech cars on the market, the company Tesla is an obvious case for connected cars. Software is featured

prominently in both the engineering and design of the car. The other proposed cases offer more typical examples of connected cars. While BMW, Nissan, and Chrysler are all popular brands, they also reflect a sufficient range from luxury to more affordable vehicles and include European, Asian, and North American brands.

The wearables present a reasonable range of products. Fitbit was a pioneer in the wearables category and represents a product specifically designed for tracking health and fitness. Smart watches do that and more. Two smartwatches were selected: the market leader, Apple, and nearest competitor, Samsung. One smart glasses product was chosen; it is also notable that Focals by North is a Canadian company (and supported by significant Innovation, Science, and Economic Development Canada (ISED) investments).[27] Consideration was given to including Google Glass, which was the first-to-market, or Apple "AR" (augmented reality), which is set to launch in the future. However, it is unclear at this stage whether these further examples are necessary or redundant. Notably, after our data was collected Google proposed to acquire Fitbit, subject to regulatory approval, and did acquire North. One stand-alone virtual reality headset was chosen. While the Oculus is not yet a mainstream product, significant growth in this subcategory of wearables is possible. Furthermore, such products could transform consumer behaviour in respect of cultural/copyright industries by fundamentally changing the ways in which consumers experience music, film and television, sporting events, and other live performances. That could have serious copyright ramifications.

For the home systems category, Nest (owned by Google) is one of the market leaders in smart home systems. For this study, we chose the thermostat, which we believe was among the company's first and remains among its most popular products. We also included the Philips smart light bulbs and the August Home smart locks. A smart camera by Arlo, a company specialised in smart security products, was later added to the sample.

In the category of home appliances, we used a reasonable range of products: a vacuum cleaner, refrigerator, washing machine, and television. The Family Hub refrigerator of Samsung and the LG laundry machine are both parts of larger ecosystems, respectively SmartThings and SmartThinQ, created by the companies to let users control all their smarts products from the same device. Both hubs also provide application programming interfaces (API) that let developers create third-party applications for the IoT market.

We selected all of the four dominant digital personal assistants available on the market at the time of our research. The products in this category are, we believe, a relatively homogenous sample in terms of product characteristics.

---

[27] Innovation, Science and Economic Development Canada, *Government of Canada supports high-growth technology manufacturing in Kitchener-Waterloo* (13 November 2018), online: Government of Canada < https://www.canada.ca/en/innovation-science-economic-development/news/2018/11/government-of-canada-supports-high-growth-technology-manufacturing-in-kitchenerwaterloo.html > .

Finally, based on our initial research, we added to our sample the AWS IoT Button manufactured by Amazon. While it cannot be classified into one of the five categories, the AWS IoT Button is an interesting, and we suspected "deviant", case because of its open infrastructure and how it lets developers create third-party applications. The button can integrate with other smart devices and has several applications such as turning on/off smart lights, opening a garage door, and control other smart appliances.

(b) Data Collection

Once the categories and list of connected products were defined, we set out to collect relevant documentation including EULAs, general Terms and Conditions documents, privacy policies and companies' websites. We specifically looked for any legal terms and conditions that addressed the smart products directly or that mentioned copyright restrictions on the integrated software. To do so, we first visited each product's webpage where documentation is usually provided on the page footer. If we did not find the relevant documentation, we contacted the companies through the available communication channels (telephone, email, chat systems). In some instances, we also contacted the person in charge of privacy practices.[28] Also, for one of the connected products[29], we were able to get the documentation while installing and registering the device with a smartphone.

Data collection was time-consuming. There were many hurdles to obtain appropriate documentation. This is indicative of poor accessibility of copyright information for Canadian consumers. We provide comments and insights on this issue in sections 3 and 4. In the end, we were able to get appropriate documentation for all of the smart products but two: BMW's ConnectedDrive system and LG's SmarThinQ laundry machine. For both products, multiple contacts and exchanges with customer service and corporate personnel officials yielded no result. We were, however, satisfied to obtain documentation for 91 % (20/22) of our sample. Information concerning the documentation can be found in the accompanying table and in Appendix A.

With EULAs, privacy policies and other documentation in hand, we built and filed a table-format questionnaire, which accompanies this article as Appendix B.

---

[28] These persons are often called "privacy officers" and their contact information can be found in the privacy policies.

[29] The Philips Hue Bulb.

3. FINDINGS

(a) Product Description and General Features

Before going over the results of the case studies, we provide below a brief description of our sample of connected products with an overview of their features.

(i) Connected cars

While automated vehicles are still years away from being driven by Canadians on a regular basis, an increasing share of cars offer low-level automation capabilities as well as multiple features powered by wireless technologies such as 4G, Bluetooth, or satellite. These features include navigation support, road assistance, and alert systems for hazards, or nearby restaurants recommendations.[30] While the government of Canada has recently looked into the security and privacy challenges generated by automated and connected vehicles,[31] it is also interesting to study them from the standpoint of copyright law.

We selected three connected cars systems: the advanced Tesla Autopilot system and two connected screen-based platforms more common in modern vehicles, the NissanConnect, and the FCA Uconnect. The main features of these systems, as well as links to their webpage, are provided in the table below.

Table 3.1 — Connected cars features

Products	**Product URL**	**Main features**	
Tesla Autopilot	https:www-w.tesla.-com/en_ca/au-topilot	- Automatic steering, braking, and acceleration - Car summoning	- Lane change suggestions
NissanConnect	https:ww-w.nissan.-ca/en/	- Emergency calling and roadside assistance	- Stolen vehicle locator - Remote door lock/unlock, horn and lights

[30] Transport Canada, *Automated and connected vehicle 101* (18 July 2019), online: Government of Canada <https://www.tc.gc.ca/en/services/road/innovative-technologies/automated-connected-vehicles/av-cv-101.html>.

[31] Senate, Standing Senate Committee on Transport and Communication, *Driving Change Technology and the future of the automated vehicle* (January 2018), online: <https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf>; Letter from The Honourable Marc Garneau (27 July 2018), online: <https://sencanada.ca/content/sen/committee/421/TRCM/reports/Minister-Garneau_GovResp_b.pdf>.

	connect	- Vehicle health report - Boundary, curfew and speed alerts - Navigation with connected and assisted search	- Smartphone connectivity and voice commands
FCA Uconnect	https:www.driveuconnect.-com/privacy-policy.hml	- Emergency calling and roadside assistance - Vehicle health report - Navigation with connected and assisted search	- Stolen vehicle locator - Remote control with Uconnect App - Compatible with Amazon Alexa - Uconnect Theater (movies and music)

The Tesla Autopilot is a driver assistance feature that "enables your car to steer, accelerate and brake automatically" with the help of sensors (cameras, radars, and ultrasonics). A driver can use the Autopilot to help them avoid collisions or automatically steer the car on highways. It is included with all new Tesla car models (S, X, and 3). Tesla also offers an advanced version called "Full Self-Driving Capability" with features such as Autopark or Summon,[32] bringing the car closer to being fully automated. These more advanced features can be installed post-purchase but come at a cost ($7,900). Tesla is also known for regularly updating its software with over-the-air updates.[33]

NissanConnect is an "integrated audio, navigation, and communication system" via a dash-mounted screen that can be installed in Nissan vehicles.[34] It offers drivers security features (roadside assistance, stolen vehicle locator, emergency calling, boundary alert, etc. . .), navigation guidance and communication features.[35] Drivers can also install apps such as Facebook or Twitter and access them through the screen. Users can link their smartphone to the platform and speak hands-free, a feature now common in many modern cars.

Our third connected car product is the Fiat Chrysler Automobiles Uconnect system. Similar to the NissanConnect, the Uconnect system offers

---

[32] Tesla Inc, *4. Autopilot* (Accessed on: 27 May 2019), online: Tesla Inc <https://www.tesla.com/en_CA/models/design#autopilot>.

[33] Over-the-air updates refer to wireless software or firmware modifications to fix errors, bring security updates or provide new features to devices. They are generally done via Wi-Fi or cellular networks. As an example, a few days after receiving criticism for its Model 3 braking distance, Tesla pushed an over-the-air update to the software reducing the braking distance by 19 feet. See Sean O'Kane, "Consumer Reports reverses course and now recommends the Tesla Model 3" The Verge (2018 May 30), online: <https://www.theverge.com/2018/5/30/17409782/consumer-reports-tesla-model-3>.

[34] Nissan Motor Co Ltd, "NissanConnect™ FAQ" (last visited 27 May 2019), online: *Nissan Motor Co Ltd* https://www.nissan.ca/en/connect/faq.html#!.

[35] Nissan Motor Co Ltd, "NissanConnect™ Features" (last visited 27 May 2019), online: *Nissan Motor Co Ltd* <https://www.nissan.ca/en/connect/features-app.html>.

communication, navigation and entertainment features via a screen. The system can receive over-the-air software updates and is compatible with Amazon's Alexa system to unlock doors, start the engine or get information on the car (tire pressure, fuel level, etc.).

(ii) Wearables

Wearables are an up-and-coming connected good category with features tailored but not limited to health and fitness markets. They include various types of smart products, generally accessories, that consumers wear. Our sample includes three smartwatches and two future-oriented products with growth prospects, a pair of smart glasses and a virtual reality headset. Their main features, as well as links to their webpages, are provided in the table below.

Table 3.2 — Wearables features

Products	**Product URL**	**Main features**	
Fitbit Charge 3	https:ww-w.fitbit.-com/en-ca/charge3	- Heart rate monitoring - Activity recognition and tracker - Sleep tracking	- Notifications from smartphone apps - Links to Fitbit App - Fitbit Pay
Apple Series 4	https.ww-w.apple.-com/ca/apple-watch-series-4	- Heart rate monitoring - Activity recognition and tracker - Fall detection - Sleep tracking - Apple Pay	- Voice activated with Siri - Built-in cellular - Built-in apps like Walkie-Talkie, Apple music or Apple Podcasts, Calendar or Maps
Samsung Galaxy Watch	https.ww-w.sam-sung.-com/global/galaxy/galaxy-watch/ >	- Heart rate monitoring - Activity recognition and tracker - Sleep tracking - Samsung Pay	- Built-in apps like My Day - Third-party apps like Spotify or Glympse - Control over IoT devices with SmartThings
North Focals	https:ww-w.by-north.-com/legal/	- Notifies, messages or alerts smartphone - Navigation directions	- Built-in Amazon Alexa - Links to smartphones

	terms-and-conditions		
Oculus Go	https.www.oculus.com/go	- Entertainment system (movies, music, video games) - Streams live events (music shows, sports events)	- Connects with other VR users - Links to Oculus App - Over 1 000 third-party apps

The Fitbit Charge 3 is a wristband that monitors heart rates, sleep quality and tracks users' fitness habits such as the number of steps per day or exercise levels. It also provides smartphone-type functions with calendar and weather apps and a mobile payment system, Fitbit Pay.

The Apple Series 4 is Apple's smartwatch launched in autumn 2018 in Canada (it has subsequently been updated by the Series 5). It offers similar fitness and health tracking features as the Fitbit Charge 3, but also features other Apple services such as Apple music or Apple podcast. It is voice-activated with Siri and has the option of built-in cellular. Recently, Health Canada has approved Apple's electrocardiogram app which monitors heartbeats and can diagnose atrial fibrillation.[36]

The third smartwatch of our sample is the Samsung Galaxy Watch that can track your heartbeat, your sleep quality, and your exercise levels. Third-party apps such as Spotify or Glympse can be installed on the watch. Interestingly, the watch also connects with the SmartThings ecosystem and lets you control your other smart devices.

The smart glasses hype subsided since Google stopped selling the Google glasses to the mass market, instead orienting its efforts towards selling them to businesses. But the future of augmented reality is still undetermined, so we included in our sample the Focals glasses by North. The glasses work with a holographic lens display of information that the user can read while wearing the glasses. While wearing them, you can receive updates, texts, or get directions to a location. The glasses also work with Amazon's Alexa. After our data collection and just before publication of this article, North was acquired by Google. Support for its current products has been wound down, and development of future products has been discontinued.

Finally, the 5th wearable of our sample is the Oculus Go virtual reality headset. VR services keep growing every year and you can now watch live concerts or sports events. The Go also enables users to watch movies or play video games, with a collection of over 1 000 applications.

---

[36] The Canadian Press, "Apple confirms ECG app for smartwatch coming in Canada but timing isn't known" CBC News (24 May 2019), online: < https://www.cbc.ca/news/business/apple-ecg-watch-1.5149352 > .

(iii) Home systems

Smart home system devices are a popular consumer category and should continue to grow in the coming years with the rise of domestic applications. They are generally controlled with a smartphone or digital assistants. They are sold on the basis they provide convenience, comfort, and security through automation and remote-control features.

Table 3.3 — Home systems features

Products	**Product URL**	**Main features**	
Nest Learning Thermostat	https://nest.com/ca/fr/thermostats/nest-learning-thermostat/overview	- Learning function and automatic programming - Remote control with the Nest App	- Location-aware - Alerts system - Energy tracking
Philips Hue Bulbs	https://www2.meethue.com/en-us/how-it-works	- Color ambiances - Remote control with the Philips Hue App rate monitoring - Location-aware and motion sensors	- Works with voice-controlled platforms - Integrates with other third-party IoT systems
August Home Smart Lock Pro	https://august.com/products/august-smart-lock-pro-connect	- Remote control with the August App - Guest access digital keys - Activity tracking - Works with voice-controlled platforms	- Location-aware - Auto-Lock - Links to August Connect Wi-Fi Bridge - Integrates with other third-party IoT systems
Arlo Pro 2	https.www.arlo.com/en-us/products/arlo-pro-2/d	- Remote access with the Arlo App - Sound and motion detection	- Works with voice-controlled platforms - Cloud storage

The Nest Learning Thermostat is a smart thermostat that will gradually learn the habits and temperature preferences of its users. It can be controlled at distance via a smartphone and can detect when a person is leaving/arriving and adjust the temperature automatically. Several energy utilities and energy efficiency organizations in Canada offer rebates when you buy them.[37]

The Philips Hue Bulbs let you create color ambiances with the Philips Hue app. It also gives a user remote control and more advanced presettings with the Hue Bridge. The Hue Bulbs can also be paired with all major digital assistants and other smart products.

The last two home systems smart products are security oriented. The August Home Smart Lock Pro can be attached to an existing deadbolt and can be opened/closed remotely with the help of a smartphone. It can auto-unlock when you arrive home and can be controlled by voice with the major digital assistants. The second product, the Arlo Pro 2, is a smart camera equipped with motion and audio detection features. You can watch live footage remotely or past recordings through the Arlo Cloud Recording feature. It also works with Amazon Alexa and Google Assistant.

(iv) Home appliances

While smart TVs have been on the market for several years, other appliances are just starting to include connectivity and automation features. Some of them are still expensive and have not reached the mass market but we should expect the smart appliances market to grow in the coming years and their prices to go down.

Table 3.4 — Home appliances features

Products	**Product URL**	**Main features**	
iRobot Roomba i7+	https://shop.irobot.ca/en_CA/roomba-vacuuming-robot-vacuum-irobot-roomba-	- Smart mapping and automatic navigation - Automatic disposal - Works with voice-controlled platforms - Links to the iRobot HOME App	- Smart mapping and automatic navigation - Automatic disposal - Works with voice-controlled platforms - Links to the iRobot HOME App

[37] See Energy Efficiency Alberta, "Online Rebates Smart Thermostats" (last visited 27 May 2019), online: *Energy Efficiency Alberta* <https://www.efficiencyalberta.ca/online-rebates/smart-thermostats/>.

	i7-plus/i755020.-html?cgi-d = ca&_-g-a = 2.903-25530.12-2940832-2.155944-5378-1992971-787.1559-445378		
Samsung Family Hub	https://www.sa-msung.-com/ca/refrigera-tors/aw1	- Built-in cameras for an inside view - Built-in food and entertainment apps	- Voice-controlled with Bixby - Control other Smart-Things devices
Sony Bravia TV	https://www.so-ny.ca/fr/electro-nics/an-droid-tv	- Android TV built-in - Voice-activated with Google Assistant	- Access to apps from the Google Store

The company iRobot has been making vacuuming robots for more than 15 years.[38] The Roomba i7 + is the latest version of its "i" series. The vacuum robot will gradually learn its surroundings by creating a visual map of rooms and obstacles. The Roomba also automatically disposes dust into the Clean Base Automatic Dirt Disposal and can be controlled with the iRobot Home app or digital assistants such as Amazon Alexa or Google Assistant.

Samsung Family Hub refrigerators are equipped with a touchscreen and cameras that let you see the inside of your refrigerator. From the touchscreen, you have access to recipes, you can manage shopping lists, shop for groceries, and many other entertainment features are available. The Family Hub also integrates with the Samsung SmartThings ecosystem and other smart devices such as smart locks and cameras that can be activated via the touchscreen.

The Sony Bravia TV comes with Android TV built-in, and a collection of apps is accessible through the Bravia TV. You can use Google Assistant to ask to watch a movie or control other smart devices linked to the Google Assistant

---

[38] iRobot Corporation, "History" (last visited 27 May 2019), online: *iRobot Corporation* < https://www.irobot.com/about-irobot/company-information/history > .

(examples include Philips Hue smart lights, Nest cameras or the iRobot Roomba).

(v) Digital assistants

Many products described above can be activated with digital voice assistants. We have included in our sample four of the major digital assistants available on the market:[39] Google Assistant, Amazon Alexa, Apple Siri, and Samsung Bixby. Three of them have been popularized through voice-controlled pods (Google Home, Amazon Echo, and Apple HomePod) while Samsung is currently working on its own AI speaker called Galaxy Home.[40] All digital assistants are also integrated with smartphones or other smart devices.

Table 3.5 — Digital assistants features

Products	**Product URL**	**Main features**	
Google Assistant (Home)	https://store.google.com/ca/product/google_home	- Queries - Voice match - Control other IoT devices	- Chromecast streaming - Voice-activated third-party apps
Amazon Alexa (Echo)	https://www.amazon.-com/dp/B07FZ8-S74R	- Queries - Hands-free calling and texting - Control other IoT devices	- FireTV streaming - Voice-activated third-party apps
Apple Siri (HomePod)	https://www.apple.com/ca/fr/homepod	- Queries - Hands-free calling and texting - Control other IoT devices	- Apple TV streaming or other Apple devices - Voice-activated third-party apps
Samsung Bixby	https://www.samsung.-com/us/explore/	- Queries - Automatic learning - Bixby Shopping - Bixby Vision	- Automatic identification and translation - Control other IoT devices

[39] A fifth one would be Microsoft's Cortana.

[40] Samsung Electronics America Inc, "Galaxy Home" (last visited 27 May 2019), online: *Samsung Electronics America Inc* <https://www.samsung.com/us/explore/galaxy-home/>.

	bixby/		

(vi) Other

The AWS IoT Button, a "cloud programmable dash button", was added to the initial sample because of its many IoT applications and how its open infrastructure lets developers or advanced users configure their own services. Examples of applications include opening your garage door, calling someone, switching on and off other smart devices, or ordering food.[41]

Table 3.6 — AWS IoT features

Products	**Product URL**	**Main features**	
AWS IoT Button	https://aws.amazon.com/iotbutton/	- Programmable - Developer-oriented	- Works through Amazon IoT Core cloud service

(b) Business Models

(i) Prices and business models

We first focus on the consumer-side of IoT business models. When selling their goods and services to consumers, IoT businesses may adopt different business models. Some will sell their products as standard electronics with an upfront one-time payment while others will turn consumers' data into premium subscription services.

In Table 4.1 below, we categorize these business models in three categories: One-Time Payment, Subscription, or Up-front fee + Subscription. We also indicate the products' prices, parent company, and headquarters.

[41] Amazon.com Inc, "AWS IoT Button" (last visited 27 May 2019), online: *Amazon.com Inc* <https://aws.amazon.com/iotbutton/>.

Table 4.1— Business models

Products	**Parent Company**	**Headquarters**	**Business Model**	**Price**[42]
Tesla Autopilot	Tesla, Inc.	California, USA	One-Time Payment	$0[43]
NissanConnect	Renault-Nissan-Mitsubishi	Japan	Subscription	$16.99 + /month
FCA Uconnect	Fiat Chrysler Automobile	Netherlands	Subscription	$14.99 USD/month
Fitbit Charge 3	Fitbit, Inc.	California, USA	One-Time Payment	$199.95
Apple Watch Series 4	Apple, Inc.	California, USA	One-Time Payment	$519 +
Samsung Galaxy Watch	Samsung Group	South Korea	One-Time Payment	$419.99 +
North Focals	North	Ontario, Canada	One-Time Payment	$599.99 +
Oculus Go	Facebook Technologies, LLC	California, USA	One-Time Payment	$269.99 +
Nest learning thermostat	Alphabet, Inc.	California, USA	One-Time Payment	$249
Philips Hue Bulb	Signify	Netherlands	One-Time Payment	$89.99 +
August Home Smart Lock Pro	Assa Abloy Group	California, USA	One-Time Payment	$229.99 USD
Arlo Pro 2	Netgear, Inc.	California, USA	Up-front fee + Subscription	$219.99 USD + $0 + /m
iRobot Roomba i7 +	iRobot® Corporation	Massachusetts, USA	One-Time Payment	$1,349.99
Samsung Family Hub	Samsung Group	South Korea	One-Time Payment	$2,999.99 +
Sony Bravia TV	Sony Corporation	Japan	One-Time Payment	$749.99 +
Google Home	Alphabet, Inc.	California,	One-Time Pay-	$129.99

[42] Prices are taken directly from the manufacturer's website. When not available, we use the price of Canadian main electronics store Best-Buy.

[43] Tesla changed its Autopilot price structure in April 2019. It is now included in new cars.

(Assistant)		USA	ment	
Amazon Echo (Alexa)	Amazon.com, Inc.	Washington, USA	One-Time Payment	$129.99
Apple HomePod (Siri)	Apple, Inc.	California, USA	One-Time Payment	$399.99
Samsung Bixby	Samsung Group	South Korea	-	-
Amazon AWS IoT Button	Amazon.com, Inc.	Washington, USA	Up-front fee + Subscription	$14.99 + USD + $0 + /m

By looking at the parent companies of each product, it is notable that the four major electronics brands (Amazon, Apple, Google, and Samsung) are heavily invested in the IoT business. Since these brands own four of the most popular digital assistants on the market, there seems to be pressure to have a sizable line-up of smart products. The value of digital assistants increases for consumers as they can control/activate more IoT goods.

We suspect that is one of the reasons major players have acquired other IoT device manufacturers in the past few years: Google bought Nest in 2014 and FitBit and North in 2020, and Amazon bought Ring in 2018. Both companies now use some these products to bundle offers to customers. For example, Google offered[44] the Google Home mini for free with the purchase of a Nest Learning Thermostat.

We find that most of the companies in our sample sell their smart products with an up-front, one-time payment. Only four companies rely on subscription-based business models or a combination of up-front fees and subscriptions. However, premium services with additional features or storage space can be found in all three categories. For example, as indicated in the previous section, Tesla drivers can activate additional features with Full Self-Driving Capability such as automated car parking and summoning for a fee of $7,900.[45] EULA terms for premium services, when they exist, are not more favourable to consumers. Copyright terms generally apply to all software, including those used to provide premium services.

Both the Nissan and the FCA have partnered with SiriusXM to offer subscription-based services. The NissanConnect will sell packages (Basic, Premium, and Premium Plus) with additional features priced at increasing monthly fees while the FCA Uconnect has a unique monthly fee. Tesla, which recently changed its price structure, now sells its newer models with the Autopilot included. Consumers who want the more complete features of Full Self-Driving need to pay an additional $7,900.

---

[44] As of June 2019.

[45] *Tesla Inc, 4*. "Autopilot" (last visited 5 June 2019), online: *Tesla Inc* <https://www.tesla.com/en_CA/models/design#autopilot>.

All wearables are sold as one-time payment products but there are some disparities in post-sale services due to their unique nature. For example, the Fitbit makes use of the fitness tracking abilities of the Charge 3 to sell Fitbit Coach, a personalized remote coaching service ($54.99/year). Both the Oculus Go and the Apple Watch Series 4 do not require subscriptions, but consumers are able to buy third-party apps or subscriptions services.

The Arlo Pro 2 camera and the Amazon AWS IoT Button are both sold with an up-front fee and a subscription plan. Arlo will offer additional features, such as better detection and increasing cloud storage space, through its Smart Arlo plans. The AWS IoT button will integrate with Amazon Web Services, which might charge a fee depending on the usage.

We also find that many of the companies in our sample will sell consumers bundles of smart products that mesh together through smart hubs. Examples of this include the security-oriented products August Home smart lock and Arlo camera which are offered together with other cameras, doorbell cameras, smart keypads, or security lights.

(ii) Third-party integration and IoT ecosystems

Central to the IoT business models adopted by companies is the interoperability of connected objects, i.e., how they communicate or control other third-party applications and devices. This is important for consumers because more interoperability can bring additional features and convenience for those who may opt to control their smart devices through a single application or hub. Below are some of the trends we observed while doing our research.

We first note that most of the products in our sample have at least some degree of interoperability where they can run third-party applications and/or be controlled by a third-party application or device. For example, the NissanConnect system hosts a series of popular applications such as Facebook, Twitter, or TripAdvisor, but can also be controlled remotely with Amazon Alexa and Google Assistant. Table 4.2 below lists third-party integrations for all of the products.

Table 4.2 — Third-party integrations

Products	Can the device run third-party apps?	Can a third-party app control the device?
Tesla Autopilot	Y	Y
NissanConnect	Y	Y
FCA Uconnect	Y	Y
Fitbit Charge 3	Y	Y
Apple Watch Series 4	Y	Y
Samsung Galaxy Watch	Y	Y
North Focals	N	Y
Oculus Go	Y	N
Nest learning thermostat	N	Y
Philips Hue Bulb	N	Y
August Home Smart Lock Pro	N	Y
Arlo Pro 2	N	Y
iRobot Roomba i7 +	Y	Y
Samsung Family Hub	Y	Y
Sony Bravia TV	Y	Y
Google Home (Assistant)	Y	Y
Amazon Echo (Alexa)	Y	N
Apple HomePod (Siri)	Y	N
Samsung Bixby	Y	N
Amazon AWS IoT Button	Y	Fully Customizable

Most of the companies in our sample will make a smartphone application freely available to control their brand of smart products. These applications are generally not compatible with other smart devices. For example, a user of the Arlo app will not be able to control their iRobot vacuum, and vice-versa.

To do so, consumers have to rely on smart hubs. This, we believe, is why we find that gradually more and more smart products are compatible with at least some the four major digital assistants (Google Assistant, Alexa, Siri, Bixby). Companies in the Home Systems and Home Appliances categories will use the ability to control smart devices with digital voice assistants as selling point to consumers.

Underlying this trend is how Amazon, Apple, Google, and Samsung[46] have each been able in recent years to consolidate their market position with their own

IoT ecosystems and IoT protocols. While they are all using the voice assistants to their advantage, their business models and the degree of openness of their systems differ in some respects.

Both Amazon and Google have positioned themselves strongly in the IoT cloud service business. Companies using the Amazon IoT Core or the Google Cloud IoT solutions will get access to advanced big data analytics features such as machine learning or predictive maintenance. Both companies offer developers software development kits to integrate connected products to their digital assistants.

Apple puts forward its own proprietary protocol, the HomeKit Accessory Protocol, that allows Apple products to communicate with third-party devices. Out of the four major IoT ecosystems, HomeKit is the least open infrastructure. Companies that distribute or sell Homekit-compatible devices need to enroll in the MFi program.[47] In our sample, we also found that many of our products were not compatible with Siri and the HomeKit protocol.

Samsung adopts a more open approach with its SmartThings ecosystem, a "programmatic interface for controlling smart devices".[48] SmartThings is a collection of tools (APIs, cloud integrations, software development) for developers who want to make their smart device SmartThings compatible. Developers can also use the Works with SmartThings label, free of charge, but have to go through a certification process.

Companies have made some efforts in recent years to open-up their systems and facilitate third-party integrations. For example, Nest announced the OpenThread protocol[49] and Google announced the Google Assistant Connect, a chip making it easier for developers to integrate Google Assistant functionalities to their devices.

(iii) Data collection and uses

The details on IoT devices' data collection and uses are provided in privacy policies. The EULA and other legal documentation will generally refer to these privacy policies for all data-related practices.

Some of the products' EULA contain limited liability clauses for the data loss following software updates. For example, the FCA Uconnect EULA states the following: "The Services involve software that we may need to change from

---

[46] We also note that Microsoft is heavily invested in the IoT market with its Azure IoT cloud service solutions.

[47] Apple Inc, "HomeKit" (last visited 5 June 2019), online: *Apple Inc* <https://developer.apple.com/homekit/>.

[48] Samsung Electronics America Inc, *Build connected IoT experiences for millions of SmartThings users*, online: Samsung Electronics America Inc <https://smartthings.developer.samsung.com/>.

[49] Nest Labs Inc, *Nest Announces Open Source Implementation of Thread* (11 May 2016), online: Nest Labs Inc <https://nest.com/ca/fr/press/nest-announces-open-source-implementation-of-thread/>.

time to time. Your Vehicle's systems also involve software that we may need to change from time to time. You agree to allow this to be done remotely without your further consent to upgrade the system operating software, fix defects or provide updated security. It is possible that such changes may affect or erase customer preferences stored on the system in your Vehicle."

We reviewed privacy policies for each of the 20 smart products. We looked specifically for practices related to the collection, use, sharing, and selling of users' data. We also looked for data access provided to users.

In general, we find that the information presented in privacy policies is of limited use for consumers both wanting to know more about their data if they use the product and to fully understand the company's business models. First, privacy policies are rarely product-specific and apply to all services provided by the companies, including their website, applications, devices, software, APIs, and all other products they manufacture. For that reason, it is often hard to know if the data collection or uses terms apply to the product or other services. Under the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[50] meaningful consent for the collection and use of personal data is required. If the consumer cannot know the terms of the data collection and use, this raises the question of whether any consent provided is valid. Below is a table with information on which the privacy policies region/country coverage and their scoping.

Table 4.3 — Privacy policies scope

Products	**Privacy policies**	
	Country or Region	**Scope**
Tesla Autopilot	North America	General
NissanConnect	Canada	Category-specific
FCA Uconnect	Canada	Category-specific
Fitbit Charge 3	Global	General
Apple Watch Series 4	Global	General
Samsung Galaxy Watch	Global	General
North Focals	North America	General
Oculus Go	North America	General
Nest learning thermostat	Canada	General
Philips Hue Bulb	Global	General
August Home Smart Lock Pro	North America	Category-specific
Arlo Pro 2	North America	General

[50] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

iRobot Roomba i7+	North America	General
Samsung Family Hub	North America	General
Sony Bravia TV	North America	General
Google Assistant	North America	General
Amazon Alexa	Canada	General
Apple Siri	North America	General
Samsung Bixby	North America	General
Amazon AWS IoT Button	North America	General

Second, terms related to the collection of data are both extensive and non-exhaustive. The data collected by companies include, but are not limited to:

- Contact information when creating an account;
- Extensive information when using the device, including records of audio conversations, location coordinates, or health data;
- Payment information when buying a product or subscribing to a service;
- Website or application usage information through the use of cookies, pixels, or similar technologies;
- Device information;
- All customer service or website (such as forums) communications;
- Friends and other contact information; and
- Other sources of information, including from public databases, social media platforms, and other third parties.

Companies will generally make the distinction between data provided by users directly, data automatically collected, and data obtained from other sources. Similarly, the ways companies use and share data with third parties are extensive and non-exhaustive.

Data uses include:

- Providing and maintaining the products and services;
- Improving products and services;
- Personalizing the products to user needs;
- Communicating with users;
- Marketing and advertisements;
- Promoting security;
- Market research and data analysis; and
- Complying with the law (audits, fraud monitoring).

Third-party sharing includes:

- Service providers for customer service, payments, customer research or satisfaction surveys;

- With third party in charge of payments;
- With affiliates and business partners;
- When required by the law or by regulatory agencies; and
- With other parties in corporate transactions (mergers or acquisition).

All details related to data uses and sharing provided by the companies apply to personal data. Indeed, only limited information is provided on the use and sharing with third parties of de-identified or aggregate data. This is important in the context of IoT because companies will use aggregated users' information to develop and sell new services.

In the same vein, the monetization of users' data is rarely mentioned in privacy policies. Only some companies specify they do not sell personal identifying information, except in the case of mergers or acquisitions. There are no direct mentions of selling aggregate or de-identified data in any of the EULAs, other terms and conditions, and policies examined. Terms covering retention periods are included in the privacy policies and are generally vague. For example, Tesla's terms say: "We will retain information we collect from or about our customers, our products, and our services for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law."

For products in our sample that are owned by a parent company, privacy policies specify that all data collected is shared within all related companies. Parent companies can then combine users' information from different sources. This underlines an important issue surrounding market power which we come back to in the next section.

We also note that the FCA Uconnect and the August Home Smart Lock Pro privacy policies involve a third party directly, respectively SiriusXM and ASSA ABLOY Limited. In these two cases, the privacy policies apply to both the company and the third party which means both are collecting and using user's data.

Finally, consumers have limited access to their data unless they communicate through legal channels. Generally, contact information and preferences will be made available through the website or the application in the account section. All other personal information collected by the devices, including all data generated while using the product, are not easily accessible. An exception would be the Google Dashboard which provides downloadable user data sets for all Google services,[51] but it does not incorporate to our knowledge data collected from Nest devices.

Privacy policies will most of the time mention that consumers do have the rights to contact the company's privacy officer (or similar official) and request all data collected on them.

---

[51] Google LLC, "Google Dashboard" (last visited 5 June 2019), online: *Google LLC* < https://myaccount.google.com/intro/dashboard?hl = en > .

(iv) Post-sale support and updates

We found that all companies in our sample provide software and security updates. These updates are free of charge. We also found no legal terms that would limit the products' usage directly. Nearly all products, except for Nest Learning Thermostat and Amazon Alexa, provide post-resale software support, free of charge as far as we were able to determine. Also, we found no explicit hardware repair or modification restrictions in any of the EULAs, other terms and conditions, and policies examined.

Regarding hardware resale or renting, we found no restrictions specified in the EULAs except for the Nest Learning product. Nest states that, "[p]urchases made on the Store are intended for end users only and are not authorized for resale". Notably, Nest's restriction on resale is found in the terms-of-sale agreement applicable for purchases through its own direct-sale retail channel; the same restriction would not appear to bind consumers purchasing Nest products through other retailers.

We address software restrictions in the Copyright section below.

(c) Legal Terms and Conditions

(i) Sales Terms, Licence Agreements

Answering questions regarding specific legal and copyright issues required us to look for appropriate legal documents containing software copyright terms and other license agreements. In many instances, this required extensive communication efforts with companies, and sometimes consulting and cross-referencing several different legal documents.

Our experience is that overall the appropriate documentation is hard to find, is a time-consuming exercise, and consumers are most likely to never get to read the copyright and other legal terms associated with their products and software. We note that this is supported by previous research. For example, in a 2016 study the Norwegian Consumer Council found similar accessibility problems concerning connected toys.[52]

First, while our methodology did not include unboxing of products, we note that sales terms, license agreements, privacy policies, and other legal documentation generally are not included with the products themselves. Rather, the only time consumers encounter these documents is when they initialize the products, generally with their smartphones, where they are provided URLs to terms and other conditions. This finding is also supported by previous smart objects analysis done at Option consommateurs.[53] We conclude from this

---

[52] Finn Lützow-Holm Myrstad, *#Toyfail: An analysis of consumer and privacy issues in three internet-connected toys* (December 2016) at 9-10, online: Forbrukerrâdet <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>.

[53] Option Consommateurs, *Enfants sous écoute: La protection de la vie privée dans*

that consumers are unlikely to be aware of any software license restrictions or other copyright obligations before they buy their products unless they do extensive online searches.

Secondly, for most of the products, the software license agreements (SLA) or end-user license agreements (EULA) are buried under general terms and conditions documentation. Documentation titles vary including: general legal webpages, Terms and Conditions (T&C), Terms of Service (ToS), and Terms of Use (ToU). Only a few companies do have product-specific license agreement documentation. We will refer to "EULA" irrespective of the product for the rest of this article.

Legal documents also often have a general scope and are not specific to applicable Canadian laws. Rather, they cover a whole range of services or contents provided by the companies and make no, or very few, distinctions between regulations of Canada and the United States.

This finding is also applicable to software licenses restrictions. Very few products in our sample have specific software license agreements. Instead, software license restrictions and other legal terms included in the legal documentation cover a broad range of services offered by the companies. It is often difficult to know if an obligation refers to the software embedded in the smart device or software embedded in other services offered by companies such as the control app.

Exceptions to this rule are Apple Watch and Apple Homepod. Indeed, Apple provides on its Canadian legal webpage[54] product-specific SLAs for its products including iPads, iPhones, Apple TVs, and Operating systems. The SLAs are also provided for each of the OS versions.

We present in the table below the legal documentation titles, country, and scope.

Table 4.4 — Scope of sales terms and license agreements

Products	**Legal documentation**		
	Title	**Country or Region**	**Scope**
Tesla Autopilot	Legal webpage	North America	General
NissanConnect	T&C	Canada	Category-specific
FCA Uconnect	ToS	Canada	General

l'environnement des jouets intelligent (March 2018) at 21-22, online: Option Consommateurs <https://option-consommateurs.org/wp-content/uploads/2018/11/oc-jouets-i-rapport-final.pdf>.

[54] Apple Inc, "Software License Agreements" (last visited 5 June 2019), online: *Apple Inc* <https://www.apple.com/ca/legal/sla/>.

Fitbit Charge 3	ToS	North America	General
Apple Watch Series 4	SLA	North America	Product-specific
Samsung Galaxy Watch	EULA	USA	Product-specific
North Focals	SLA	North America	Product-specific
Oculus Go	ToS	North America	General
Nest learning thermostat	EULA	Canada	General
Philips Hue Bulb	ToU	North America	Category-specific
August Home Smart Lock Pro	EUA	North America	General
Arlo Pro 2	ToS	North America	Category-specific
iRobot Roomba i7+	EULA	North America	General
Samsung Family Hub	EULA	North America	General
Sony Bravia TV	EULA	North America	Category-specific
Google Assistant	ToS	North America	General
Amazon Alexa	ToU	North America	General
Apple Siri	SLA	North America	Product-specific
Samsung Bixby	EULA	North America	General
Amazon AWS IoT Button	T&C	North America	Product-specific

Most of the time, EULAs are on an "all or nothing" basis, which means consumers must agree to all legal terms and obligations or otherwise should not use the product. For example, the iRobot i7+ EULA will specify that: "[i]f you do not agree to the terms of this EULA, you may not use the product software and you may choose to promptly return the product for a refund of the product purchase price by contacting the retailer at which you purchased the product or iRobot at the address below".

Many of the products rely in part on Open source software which might have their own SLA.[55] For example, the Nest Learning Thermostat uses over a

[55] Terms with mentions of the use of open software include: Tesla Autopilot, Apple Watch, North Focals, Nest learning thermostat, August Home Smart Lock Pro, Arlo Pro 2, iRobot Roomba, Sony Bravia TV, Google Assistant, Apple Siri, and all Samsung products.

hundred open source software codes[56] and its EULA states that "[c]ertain items of software included with the Product Software are subject to "open source" or "free software" licenses ("open source software"). Some of the open source software is owned by third parties. Open source software is not subject to the terms and conditions of this EULA. Instead, each item of open source software is licensed under the terms of the end user license that accompanies such open source software". Companies will generally, but not all the time, provide links to the open software licenses within the EULA or on their website.

Companies will generally, but not all the time, provide links to the open source software licenses within the EULA or on their website. Note that our analysis of EULA terms did not extend to the separate SLA of open source software.

(ii) Copyright

We looked in the EULAs for copyright terms covering the services, products or any parts of them. We present the results in the table below.

Table 4.5 — Copyright terms

Products	**Are there general copyright terms?**	**Are there copyright terms regarding software?**
Tesla Autopilot	Y	N
NissanConnect	N	Y
FCA Uconnect	Y	Y
Fitbit Charge 3	Y	Y
Apple Watch Series 4	Y	Y
Samsung Galaxy Watch	Y	Y
North Focals	Y	Y
Oculus Go	Y	Y
Nest learning thermostat	Y	Y
Philips Hue Bulb	Y	Y
August Home Smart Lock Pro	Y	Y
Arlo Pro 2	Y	Y

[56] Nest Labs Inc, "Open Source Compliance" (last visited 6 July 2019), online: *Nest Labs Inc* <https://nest.com/ca/legal/compliance/>; Other examples include: North Inc, *3rd Party Licenses* (2 January 2019), online: North Inc <https://www.bynorth.com/legal/3rd-party-licenses> and August Inc, *August Doorbell Cam Notices and Licenses* (29 October 2018), online: August Inc. <https://cdn.shopify.com/s/files/1/1354/7835/files/August-Doorbell-Cam-Notices-and-Licenses_00ac0131-d4a4-43ff-bc7f-3d643c6ea724.pdf?6692232982540496972>.

iRobot Roomba i7+	Y	Y
Samsung Family Hub	Y	Y
Sony Bravia TV	Y	Y
Google Assistant	Y	Y
Amazon Alexa	Y	Y
Apple Siri	Y	Y
Samsung Bixby	Y	Y
Amazon AWS IoT Button	Y	Y

Most of the products in our sample contain copyright terms of general nature (19/20). An example is the Oculus Go statement on Ownership and Intellectual Property. "Unless otherwise indicated, the Services are the property of Oculus or our licensors and are protected by copyright, trademark and other laws of the United States and foreign countries. You will not remove, alter or obscure any copyright, trademark, service mark or other proprietary rights notices incorporated in or accompanying the Services."

We looked specifically for copyright terms regarding each product's software. Again, nearly all of the EULAs contained terms concerning the software (19/20). Most of the time, software copyright terms can be found at the start of EULAs where companies state that they grant consumers a license to use the software and list all limitations, which are described in detail below.

The product where we could not find software copyright terms is the Tesla Autopilot. A possible explanation is that we did not have access to all the legal documentation. For example, we did not have access to the Motor vehicle purchase agreement (MVPA), a document that consumers often sign before they buy a car. Internet searches suggest that this might be the case for the Tesla Autopilot.

Note that we also found ambiguous copyright terms concerning user's data that would be generated through Amazon Alexa. Indeed, Amazon claims that "data compilations [. . .] is the property of Amazon.ca or its content suppliers, and is protected by Canadian and international copyright laws".[57] It is unclear whether Amazon refers to data gathered from its users or data that the company generates and shares with its users.

Copyright license restrictions restrictions are most often encountered in EULAs under "License restrictions" sections. We also looked for any exceptions to those restrictions. For example, are users allowed to circumvent technological protection measures (TPM) to repair or refurbish their product/software

[57] Full quote: "All content included in or made available through any Amazon.ca Service–such as text, graphics, logos, button icons, images, audio clips, digital downloads, data compilations, and software–is the property of Amazon.ca or its content suppliers, and is protected by Canadian and international copyright laws. The compilation of all content included in or made available through any Amazon.ca Service is the exclusive property of Amazon.ca and protected by Canadian and international copyright laws."

themselves? The *Copyright Act* gives rights-holders the right to prevent the circumvention of TPMs protecting their software. The *Copyright Act* also provides exceptions to allow users to circumvent those TPMs under certain limited circumstances, e.g. to ensure interoperability of software.[58]

It is important to note that the research project did not examine the question of whether the restrictions outlined in manufacturers' EULAs are consistent or not with Canada's *Copyright Act*, or with other key laws and jurisprudence in Canada. Rather, the research project sought to describe the main restrictions without commenting on whether they would be found to be legally enforceable. The results are presented in the table below.

Table 4.6 — Copyright terms - Restrictions and exceptions

Products	**Are there restrictions on resale or renting?**	**Are there restrictions on modification or repairs?**	**If yes, can the user modify, repair, or refurbish the product themselves?**	**If yes, can any third-party repair, modify, or refurbish the product?**	**If yes, can the user circumvent any TPMs?**
Tesla Autopilot	N	Y	N	-	-
NissanConnect	Y	Y	-	-	-
FCA Uconnect	Y	Y	-	-	-
Fitbit Charge 3	Y	Y	N	N	N
Apple Watch Series 4	Y	Y	-	-	-
Samsung Galaxy Watch	Y	Y	-	-	-
North Focals	Y	Y	-	-	-
Oculus Go	Y	Y	N	N	N
Nest learning thermostat	Y	Y	N	N	-
Philips Hue Bulb	Y	N	-	-	N
August Home Smart Lock Pro	Y	Y	N	N	-
Arlo Pro 2	Y	Y	N	N	N
iRobot Roomba	Y	Y	-	-	-

[58] *Copyright Act*, RSC 1985, c C-42, s 41.

i7+					
Samsung Family Hub	Y	Y	-	-	-
Sony Bravia TV	Y	Y	-	-	N
Google Assistant	Y	Y	-	-	-
Amazon Alexa	Y	N	-	-	-
Apple Siri	Y	Y	-	-	-
Samsung Bixby	Y	Y	-	-	-
Amazon AWS IoT Button	Y	Y	-	-	-

The restrictions in software licenses are often extensive. For example, Fitbit will state that "[y]ou will not use, sublicense, copy, adapt, modify, translate, disclose, prepare derivative works based upon, distribute, license, sell, rent, lease, assign, transfer, publicly display, publicly perform, transmit, broadcast, or otherwise exploit the Fitbit Content, Fitbit Service or any portion thereof (including any third-party software), except as expressly permitted in these Terms".

In all EULAs containing copyright terms regarding software, users are prohibited from selling or renting the software. The clauses do not make clear whether they purport to prohibit selling or renting of the software separately from the device, or whether they in effect prohibit selling or renting the device itself which includes the software. Thus, consumers are unlikely to know in advance, even if they had meaningful access to the terms, which interpretation was intended by the seller or how such a clause would be interpreted by the courts.

However, some companies allow a one-time transfer of ownership to another user, attached to some restrictions:

- Apple HomePod: "*You may, however, make a one-time permanent transfer of all of your license rights to the HomePod Software to another party in connection with the transfer of ownership of your HomePod, provided that: (a) the transfer must include your HomePod and all of the HomePod Software, including all its component parts and this License; (b) you do not retain any copies of the HomePod Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the HomePod Software reads and agrees to accept the terms and conditions of this License*."
- Samsung Watch: "*You may not transfer this EULA or the rights to the Samsung Software granted herein to any third party unless it is in connection with the sale of the Product which the Samsung Software accompanied. In such event, the transfer must include all of the Samsung Software (including all component parts, the media, and printed materials, any upgrades, this*

EULA) and you may not retain any copies of the Samsung Software. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the Samsung Software must agree to all the EULA terms."

- Sony Bravia TV: "*In addition, you may not rent, lease, sublicense, or sell the Sony Software, but you may transfer all of your rights under this EULA only as part of a sale or transfer of the Sony Product provided you retain no copies, transfer all of the Sony Software (including all copies, component parts, any media, printed materials, all versions and any upgrades of the Sony Software, and this EULA), and the recipient agrees to the terms of this EULA. Sony and its Third Party Licensors retain all rights that this EULA does not expressly grant to you.*"

Similarly, we also found modification restrictions on nearly all of the products licensing their software (17/19). Similar restrictive terms to what would amount to a software modification include "adapt", "prepare derivative", "decompile", "reverse compile", "reverse engineer", "disassemble", "decrypt", and "attempt to derive the source code". The North Focals EULA also includes "enhance" and "improve" restrictions.

We did not encounter specific "repair" or "refurbish" software license restrictions in EULAs. However, the modification or similar restrictions on software license mentioned above are likely to amount to repair restrictions since the user would need to modify parts of the software and, likely, access to the object code, to correct any errors. Some companies provide information on how consumers can repair their products (e.g. Apple and Fitbit[59]), including information on "authorized retailers".

We did find several companies that specified the legal warranty is void if there are any unauthorized repair attempts by either users or third parties. These companies are Tesla, Fitbit, Oculus, Nest, August, and Arlo.

Regarding TPMs, most companies (13/20) do not include specific TPM circumvention restrictions in EULAs. The five products that do specifically prohibit TPM circumvention by contract (in addition to the prohibitions already contained in the *Copyright Act*[60]) are the Fitbit Charge 3, the Oculus Go, the Philips Hue Bulbs, the Arlo Pro 2, and the Sony Bravia TV. Some EULAs, such as Fitbit's and Arlo's, reference the possibility that certain acts of circumvention may be legally permitted. Others, such as Oculus's and Philips's, do not mention the possibility of legal circumvention, raising questions about whether or not their contracts purport to override the *Copyright Act*. For example:

- Fitbit Charge 3: "*Except to the extent permitted by law, you may not perform, attempt to perform, or encourage or assist others in performing any of the following while accessing or using the Fitbit Service: [. . .] (5)*

---

[59] Fitbit Inc, "Authorized Retailers" (last visited 5 June 2019), online: *Fitbit Inc* < https://www.fitbit.com/sg/legal/authorized-retailers > .

[60] *Copyright Act*, RSC 1985, c C-42, s 41.

circumvent any technological measure implemented by Fitbit or any of Fitbit's providers or any other third party (including another user) to protect the Fitbit Service".

- Oculus Go: "*By accessing or using the Services, you agree that you will not: [. . .] circumvent or attempt to circumvent any filtering, security measures or other features designed to protect the Services, or third parties*".
- Philips Hue Bulbs: "*You agree to [. . .] not to circumvent or attempt to tamper with the security of or disable any of the Products or Services or other end user devices*".
- Arlo Pro 2: "*Arlo may terminate the accounts of users of any Arlo service or software who infringe the copyrights, trademarks, or intellectual property rights of others. In addition, steps intended to defeat or bypass security measures designed to prevent intellectual property infringement may be illegal under U.S. law or comparable foreign laws. Arlo may terminate the Arlo accounts of users who develop or use methods to defeat or bypass such security measures and may take any other necessary or appropriate action to prevent infringement of intellectual property holders' rights*".
- Sony Bravia TV: "*Sony and its Third Party Licensors retain all rights that this EULA does not expressly grant to you. You shall not (a) bypass, modify, defeat, or circumvent any of the functions or protections of the Sony Software or any mechanisms operatively linked to the Sony Software*".'

Finally, we looked for restrictions on interoperability with other devices, on the use of assistive technologies for persons with disabilities and on limited liability disclaimers. Results are presented in Table 4.7 below.

Table 4.7 — Copyright terms — Interoperability, assistive technologies, and limited liability

Products	**Are there restrictions on interoperability with other devices**	**Are there accommodations for the use of assistive technologies for persons with disabilities?**	**Are there disclaimers of limited liability for product defects, including software malfunction?**
Tesla Autopilot	N	N	Y
NissanConnect	N	N	Y
FCA Uconnect	N	N	Y
Fitbit Charge 3	Y	N	Y
Apple Watch Series 4	Y	N	Y
Samsung Galaxy Watch	N	N	Y
North Focals	N	N	Y
Oculus Go	N	N	Y

Nest learning thermostat	N	N	Y
Philips Hue Bulb	N	N	Y
August Home Smart Lock Pro	N	N	Y
Arlo Pro 2	N	N	Y
iRobot Roomba i7 +	N	N	Y
Samsung Family Hub	N	N	Y
Sony Bravia TV	N	N	Y
Google Assistant	N	N	Y
Amazon Alexa	N	N	Y
Apple Siri	Y	N	Y
Samsung Bixby	N	N	Y
Amazon AWS IoT Button	N	N	Y

We found restrictions on interoperability with other devices for three products, although the restrictions are not explicit
:

- Both Apple Watch Series 4 and Homepod EULAs include limitations to the use of Apple proprietary content with third-party devices, accessories or applications in conjunction with the Apple Watch and Homepod. For example, the Homepod EULA states that, "[t]his License does not grant you any rights to use Apple proprietary interfaces and other intellectual property in the design, development, manufacture, licensing or distribution of third party devices and accessories, or third-party software applications, for use with HomePod. Some of those rights are available under separate licenses from Apple". These "separate licenses" include Apple Made for iphone/iPod/iPad (MFi) program.[61]
- In the Fitbit Charge 3 EULA, Fitbit states that "[y]ou may not connect to the Fitbit Service with any device that is not manufactured, distributed, or sold by Fitbit itself or through its authorized resellers or agents (such as a knock off or counterfeit version of a Fitbit device); otherwise intends to resemble or purports to be a Fitbit device; or any unauthorized application or third party connection."

We found no accommodations for the use of assistive technologies for persons with disabilities. It should be noted that Canada's *Copyright Act* includes exceptions to copyright infringement for persons with perceptual disabilities and exceptions to permit circumvention of TPMs, including the provision of services and devices to permit circumvention for persons with perceptual disabilities.[62]

---

[61] Apple Inc, *MFi Program* (Accessed on: 5 June 2019), online: Apple Inc <https://developer.apple.com/programs/mfi/>.

Finally, documentation of all products contains limited liability disclaimers, including on software. Here are a few examples:

- Error-free data, uninterrupted or problem-free service (NissanConnect);
- Any damages arising from installation, repair or maintenance of the software (FCA Uconnect);
- Accuracy, reliability, availability, effectiveness, or correct use of information users receive (Fitbit Charge 3);
- Any damages of any kind arising out of, or relating to the use of the product, the inability to use the software, including but not limited to damages caused by or related to errors, omissions, interruptions, defects, delay in operation or transmission, computer virus, failure to connect, network charges, in-app purchases, and all other direct, indirect, special, incidental, exemplary, or consequential damages even if the company has been advised of the possibility of such damages (Samsung Galaxy Watch);
- Any damages relating to the use of the software, users should accept all risks (North Focals); and
- Any and all loss, liability, or damages, including to the HVAC system, plumbing, home, product, other peripherals connected to the product, computer, mobile device, and all other items and pets in your home (iRobot i7+).

Some of the EULAs note that the limited liability disclaimers might not apply in certain states/provinces. These include NissanConnect, FCA Uconnect, Fitbit Charge, Focals North, Oculus Go, Nest Thermostat, August Smart Lock Pri, Arlo Pro 2, iRobot Roomba, Samsung Family Hub, and Sony Bravia TV. This is because jurisdictions like Quebec have consumer protection laws that do not allow for limitation to legal warranties.[63]

The Oculus Go warranty will for example specify that "[i]f you are a consumer subject to the QCPA, the exclusion of warranties contained in the immediately following paragraph do not limit your rights and remedies under the Quebec Consumer Protection Act, including the right to make a claim under any of the statutory warranties provided under sections 34 to 54 of such statute". Generally, companies simply mention, like August, that "You may also have other legal rights that vary by state, province or jurisdiction".

4. ANALYSIS OF FINDINGS AND RECOMMENDATIONS

Our analysis of the legal documentation of connected objects identifies several copyright related restrictions. However, additional legal analysis is required to better understand the impacts of these restrictions on consumers and the IoT. Our study also brings to light several issues beyond copyright that merit

---

[62] *Copyright Act*, RSC 1985, c C-42, s 32.

[63] *Consumer Protection Act*, CQLR c P-40.1, ss 34-54.

consideration, such as competition, data portability, and privacy. We present below our main findings as well as a series of recommendations we believe would help strengthen consumers' confidence and ability to make informed choices in the IoT market.

Finding #1: Obtaining legal information on smart products, including software license restrictions and other copyright limitations, is an extremely difficult and time-consuming exercise. As a result, consumers are unlikely to have any knowledge of post-sale restrictions or limited liabilities before they buy connected objects.

Our methodology, which revolved around legal documentation analysis, turned out to be challenging due to the difficulty of obtaining the appropriate documents. Extensive contacts with manufacturers, both within legal and customer service communication channels, were required but often led to unhelpful answers. While we did not collect data on consumers' actual or perceived experiences with EULAs, insights were gleaned from our methodology and first-hand experience. A team consisting of qualified experts[64] facing these challenges speaks to the problems facing average consumers.

This is an important finding as manufacturers not providing adequate disclosure of material information can create competition and other policy concerns. Consumers need sufficient information to assess competing products in order to make informed purchasing decisions. For example, consumers may not wish to purchase a product with terms and conditions that require them to surrender control over personal data or contractually forego their right to take advantage of an exception under copyright law. Furthermore, this lack of information prevents consumers from providing their informed consent for the collection and use of personal data, as required under (PIPEDA).[65]

Consumers have to agree to terms and conditions that are generally located at the bottom of companies' webpage or buried inside a legal web section. Consumers are then unlikely to know about any legal obligations regarding their smart products, such as copyright software restrictions before they buy them unless they do extensive research beforehand. The only time a consumer is presented any EULA terms is during the initialization of the smart product.

Very few products in our sample have specific software license agreements, the Apple products being noticeable exceptions. Instead, software license restrictions and other legal terms included in the legal documentation cover a broad range of services offered by the companies. It is sometimes difficult to know if an obligation refers to the smart device or other services offered by companies. This level of specificity associated with Apple products may present the inverse problem to the generality of other companies' EULAs; consumers

---

[64] A law professor, a law student, and an economist focussed on consumer-affairs.

[65] PIPEDA, *supra* note 50.

may be overwhelmed by voluminous and potentially different agreements for similar products.

Previous critiques of end-user license agreements, including consumer advocacy groups, have focussed on the non-negotiability of the terms and conditions (i.e. take-it-or-leave-it) as well as the complexity of legal jargon (i.e. language, length, etc.).[66] Our research suggests a more fundamental problem of a lack of access to the governing terms and conditions. Based on our own experience, consumers may not be able to *find*, let alone *understand*, let alone *negotiate* the contracts.

Finding #2: The analysis of business models shows interoperability of platforms *within* an ecosystem of third-party devices and applications, but restrictions that limit interoperability *across* ecosystems. This market segmentation favors Amazon, Apple, Google, and Samsung, which have significant influence over smaller smart device makers.

Amazon, Apple, Google, and Samsung have built a strong presence in the IoT market in the past few years. Each put forward their own ecosystem of IoT protocols, applications, and services. They also have increased their presence in the IoT devices' markets with acquisitions of other smart products businesses, as demonstrated by Google's acquisition of Fitbit (smart watches) and North (smart glasses).

Underlying industry trends is the centrality to IoT of digital voice assistants. Each of the big four companies uses digital assistants as an advantage over competing smart device makers. This, in turn, creates incentives for other companies to make sure their devices are compatible with the four ecosystems.

While we see this kind of third-party integrations taking form between security-oriented product manufacturers and Google or Amazon ecosystems, we see more interoperability barriers *across* ecosystems. This is especially true for Apple and its HomeKit IoT protocols. For example, at the time of publication of this article it is impossible for a HomePod user to ask Siri, owned by Apple, to control a Nest thermostat, owned by Google.

The creation of these smart hubs has the advantage of being convenient for customers who might prefer to limit the number of applications they use to control their smart products. But it also positions these four companies favourably over smaller device makers. Amazon and Google are also heavily

---

[66] A study done by the Canadian Marketing Association in 2018 found that Canadians do not read privacy policies, or only parts of them, because of the length, the complexity or lack of choice. Canadian Marketing Association, *Canadians want user-friendly information about privacy policies* (25 January 2018), online: Canadian Marketing Association <https://www.the-cma.org/about/blog/canadians-want-user-friendly-information-about-privacy-policies>. In 2016, the Norwegian Consumer Council showed it took more than 30 hours to read the terms and conditions of smartphone apps used by the average Norwegian. BBC News, "Norway consumer body stages live app terms reading" *BBC News* (25 May 2016), online: <https://www.bbc.com/news/world-europe-36378215>.

invested in selling cloud services to IoT businesses, creating further incentive for companies to use their ecosystems.

We see some trends towards adopting more open protocols and facilitating third-party integrations. There is market pressure to do so as companies have strong incentives to maximize their number of users. However, IoT market segmentation should continue as makers of digital voice assistants consolidate their position. The growing size of IoT companies and consolidation in the industry are not necessarily problematic *per se*, unless there is anti-competitive behaviour.[67] Our observations about the nature of IoT products and services, and the terms and conditions specified in EULAs associated with their use, suggest that further investigation of this topic may be warranted.

Finding #3: Moving personal data from one platform to another is virtually impossible for the average consumer. Limited data portability is restricting consumer choices and raises concerns about competition in a sector highly dependant on data to bring new and innovative services to market. Data portability can also act as a privacy enhancing mechanism because it provides consumers with more transparency and control over their data.

Smart devices in our sample collect and transfer a vast amount of sensitive personal data, in addition to all data points collected by the companies from other sources such as social media. Indeed, our review of privacy policies shows how extensive data collection is. EULAs examined provide very limited information about how the data is used (e.g. combined with other sources, for what purpose, and whether they are shared with, or sold to, third-parties). Some products (e.g., Facebook's Oculus and Google Home) do have privacy policies stating that the companies use data from other services provided by other companies, but it is practically impossible to know which datasets they combine and for what purpose.

The only recourse consumers have if they want to get their hands on their personal data collected from smart devices is through legal channels that are specified in privacy law requirements. This is highly impractical and time-consuming, and consumers are most likely unaware of their right to access their personal data.

This limits significantly how consumers can move from one company to another. Companies can also benefit from consumer inertia, a well-documented phenomenon in the computer business where the costs for consumers to move from one ecosystem to another is high, especially if they benefit from free services.

Limited data portability also has an important implication for competition in an era where new services are emerging thanks to advanced data analytics. This issue is also reinforced by the substantial influence companies like Amazon or Google have. As we've seen in privacy policies, companies share collected data

---

[67] Competition Bureau, "Abuse of Dominance Enforcement Guidelines" *Government of Canada* (7 March 2019); *Competition Act*, RSC 1985, c C-34.

throughout their services. This means that Google can merge personal data obtained from the Nest devices, its Google Search engine, and its Google Maps service, giving the company powerful insights to improve products' quality, develop new services, or personalize users' experience. Generally, data portability can promote consumer choice and competition[68] and, therefore, is a topic that may warrant deeper analysis in the specific context of IoT products and services.

The extent to which companies monetize data from smart devices is difficult to know from reading the legal documentation. Privacy policies cover personal data but are very limited with respect to aggregate or anonymized data.

The issue of data portability should be increasingly important as the data collected from smart devices is more and more sensitive. An example is how the recently released in Canada Apple electrocardiogram application could be used by both private and public health services. With this application, each heartbeat is recorded, and the resulting waveform can be shared with doctors and help detect serious heart problems such as arrhythmia.

Finally, as highlighted in Canada's Digital Charter[69] and suggested by ISED in its proposals to modernize PIPEDA[70], the ability for consumers to move their data from one company to another can help them better understand which personal data is collected and how companies use them. It would enhance consumers' control over their personal data and desired degree of privacy.

Finding #4: Software licensing is now common practice across smart device manufacturers. Licenses come with important restrictions, including limiting consumers' ability to resell and modify software. Companies also include limited liability disclaimers in case of software malfunction. Implications for issues such as "right to repair" or products' obsolescence could be important but depend ultimately on if and how companies trigger the licenses legal clauses, and whether the clauses are consistent with Canadian law.

---

[68] See Competition Bureau Canada, *Technology-led innovation in the Canadian financial services sector* (14 December 2017), online: Government of Canada <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04322.html>; Competition Bureau Canada, *Submission by the Interim Commissioner of Competition to the Department of Finance Canada - Review into the merits of open banking* (11 February 2019), online: Government of Canada <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04416.html>; Ctrl-Shift, *Data Mobility: The personal data portability growth opportunity for the UK economy* (2018), online: Department of Digital, Culture, Media & Sport - Government of the United Kingdom <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf>.

[69] Innovation, Science and Economic Development Canada, *Canada's Digital Charter: Trust in a digital world* (25 June 2019), online: Government of Canada <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.

[70] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age* (21 May 2019), online: Government of Canada <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html>.

Nearly all EULA or similar legal documents we consulted contained specific copyright terms on software licenses, although the language used is sometimes ambiguous and often encompasses many services. These licenses give consumers the right to use the software with attached restrictions. These restrictions are exhaustive and include:

- Restrictions on sale or resale of software;
- Restrictions on modification or reverse engineering of software;
- Restriction on commercial uses or distribution.

Limited liability clauses on software malfunctions are also found for all products. Consumers are even told they "should accept all risks" for any software damages (North Focals). Such limitations may be illegal under certain consumer protection laws, such as the Quebec's *Consumer Protection Act*. Some products also include void warranty clauses if software repairs are done by either the owner or a third party, and some products also include anti-circumvention rules to TPMs.

Do these restrictions limit the rights of consumers to repair their smart products in case of software malfunction? On one hand, we did not encounter specific repair restrictions or any usage limitations clauses. On the other hand, given the extent to which companies limit software modifications and any liabilities to software damages, it does seem to provide very restrictive rights to consumers.

It ultimately depends on if, and how, companies will enforce these clauses. There have been examples in the past, especially in the United States. Ford sued Autel in 2014 for providing consumers with a diagnoses tool that circumvented Ford's software.[71] More recently, Adobe informed some of its users they were "no longer licensed" to use a previous software version.[72] Companies might face a backlash from consumers. As a John Deere representative said to a CBC journalist, "[w]e reserve that right [to pursue legal action] but we are more focused on wanting to ensure that the customer experience is right".[73]

This research did not examine the question of whether the restrictions on use provided by manufacturers' EULAs are consistent or not with Canada's *Copyright Act*, or with other key laws and jurisprudence. Rather, the research

---

[71] Russell Brandon, "Automakers are trying to stop you from hacking your car" *The Verge* (24 April 2015), online: < https://www.theverge.com/2015/4/24/8490359/general-motors-eff-copyright-fight-dmca > .

[72] Karl Bode, "Adobe Tells Users They Can Get Sued for Using Old Versions of Photoshop" *Vice* (14 May 2019), online: < https://www.vice.com/en_us/article/a3xk3p/adobe-tells-users-they-can-get-sued-for-using-old-versions-of-photoshop > .

[73] "Saskatchewan farmer hacks his 'smart' tractor to avoid costly dealer fees" (27 March 2017) (radio), online: *CBC Radio* < https://www.cbc.ca/radio/asithappens/as-it-happens-monday-edition-1.4042503/saskatchewan-farmer-hacks-his-smart-tractor-to-avoid-costly-dealer-fees-1.4042504 > .

project sought to describe the main restrictions without commenting on whether they would be found to be legally enforceable. What is certain is how it is almost impossible to conclude definitively before purchasing an IoT product what limits to a consumer's use of the product will be. Understanding consumer rights to repair or resell requires conclusions based on a combination of documents, including the sales agreement, software license, and warranty conditions. Even then, the language used is so ambiguous that average consumers will have difficulty determining if they can, or cannot, repair the product they purchased, including the software associated with it.

Based on these findings, we make the following recommendations. The Government of Canada and the provincial governments should take appropriate steps to improve the accessibility of legal information on smart products for consumers. These steps should include:

- Develop measures relative to the information provided to consumers in the mobile application environment, and make sure the legal information is concise, comprehensible and easily accessible.
- Consider standardized copyright, data, privacy or other labeling approaches as suggested by the *Canadian Multistakeholder Process: Enhancing IoT Security initiative*[74] to help consumers make informed choices when they buy connected objects. While label standards focus on security and privacy concerns, it should also consider the inclusion of copyright limitations.
- Raise consumer awareness of these labels and, more generally, promoting consumer education on IoT issues discussed in this research. Education campaigns should also help increase consumers' understanding of legal contracts.

To foster competition and ensure consumers have the ability to switch from one IoT ecosystem to another, we also suggest governments should:

- Actively promote the adoption of open data standards. Initiatives exist,[75] but open data standards have not yet been adopted by IoT companies. Acknowledge that individuals have an explicit right to personal data mobility.
- Actively promote the use of open IoT protocols.
- Closely monitor antitrust law discussions happening in the United States and in Europe. These discussions include proposals to break data

---

[74] Internet Society, *Canadian Multistakeholder Process: Enhancing IoT Security - Final Outcomes and Recommendations Report* (2018), online: Securing the Internet of Things < https://iotsecurity2018.ca/wp-content/uploads/2019/05/Enhancing-IoT-Securit-Report-2019-Final-EN.pdf > .

[75] Data Transfer Project, "Data Transfer Project" (last visisted 10 June 2019), online: *Data Transfer Project* < https://datatransferproject.dev/ > .

monopolies by imposing obligations on big companies to share data with smaller companies.[76] Antitrust remedies require careful consideration "to get it right" and must be tailored for Canada.

Portability and interoperability concerns require but also go beyond the revision of the *Copyright Act*. Canada's Digital Charter[77] offers insights on modifications to PIPEDA that would provide consumers with more choice and transparency, as well as increasing competition in the IoT market. For example:

- Acknowledge that individuals have an explicit right to personal data mobility.
- Define de-identified data (or pseudonymized data) and increase transparency on how companies monetize consumers' data and share aggregate data with third parties.
- Increase the role and powers of the Privacy Commissioner, including the possibility to investigate and audit.
- Adopt penalties for companies that attempt to re-identify data.

We also urge that the INDU Committee's relevant recommendations,[78] including Recommendations 18 and 19 regarding the fair dealing,[79] TPMs and the right to repair lawfully acquired devices be taken seriously, given that our study suggests INDU's concerns are well founded. We recommend that the Government of Canada undertake further analysis to determine whether the terms and conditions we identify as prevalent in the Canadian IoT marketplace are enforceable under Canadian federal and provincial laws, and if so or if not, what policy responses are possible and appropriate.

---

[76] Angela Chen, "Making big tech companies share data could do more good than breaking them up" MIT Technology Review (6 June 2019), online: < https://www.technologyreview.com/s/613629/making-big-tech-companies-share-data-could-do-more-good-than-breaking-them-up/ > .

[77] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age* (21 May 2019), online: Government of Canada < https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html > .

[78] House of Commons, Standing Committee on Industry, Science and Technology, *Statutory Review of the Copyright* Act (3 June 2019) at 69-72. online: < https://www.ourcommons.ca/Committees/en/INDU/StudyActivity?studyActivityId=9897131 > .

[79] Implementing Recommendation 18 would help address several problems identified in our study, such as dealing with embedded software fairly for purposes such as protecting privacy, ensuring interoperability, or repairing devices. It is arguable although unclear under which allowable purpose or purposes such activities might presently fall. Permitting such activities via an illustrative rather than exhaustive list would increase the flexibility of the Act to address consumers' fair dealings now and similar practices that may emerge in the IoT's future. It would promote competition and protect consumers by permitting these activities to be done by an individual or a third-party, e.g. an independent repair shop, who can rely on the individual's purpose.

5. CONCLUSION

The points of views expressed by stakeholders throughout the consultations organized by the INDU Committee show a great diversity in opinions on how to modernize the *Copyright Act*. Balancing the interests of copyright owners and users thus requires an understanding of industry-practices, trends in technologies, as well as the states and prospects of economies and digital markets. In this regard, we hope that our findings will help the Government of Canada's consideration of INDU's report and recommendations, and help it to inform consumers about the smart use of IoT devices.

Our research was based on the collection and analysis of IoT-related consumer contracts. We believe further research could also provide useful insights and help grasp the impacts of the growing IoT market. Several important issues and questions have become apparent from this research.

First, research does not assess, or draw conclusions about, the legality of the terms and conditions in the contracts we identified. Further research would be required to fully understand how these contracts affect consumers. Aspects of that work could involve comparisons across jurisdictions, both within and outside Canada. For example, in October 2018 the Library of Congress and the U.S. Copyright Office enacted exemptions under the *Digital Millennium Copyright Act* (DMCA) to allow for legal circumvention of digital locks on electronic devices for the purpose of repairs.[80] However, we note that the U.S. Copyright Office emphasized that there is doubt about whether the new exemptions would apply to third parties hired to do a repair.[81] It may be appropriate to examine the impact this decision has had on consumers' vis-à-vis IoT devices. Also, the limited liability clauses we encountered suggest a civil law analysis could help determine whether terms and conditions imposed on consumers are legal.

Second, we believe the issues could be better understood through analysis from multiple different perspectives. For example, in terms of competition policy, consumer choice is a powerful driver of competition and innovation. While TPMs serve to protect intellectual property, they can also limit the ability of independent repair shops to effectively perform repairs, even with the exceptions outlined in the *Copyright Act* that allows circumvention of TPMs in certain circumstances. Independent repairers can offer consumers a choice of repair services at greater convenience. They can also better serve rural and remote customers if there is no manufacturer-authorized repair service provider in their community, as those customers may be forced to travel to a major town or city to get their product serviced. Using licensing restrictions to prevent

---

[80] *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies* 83 Fed Reg 54010 (2018) (to be codified at 37 CFR).

[81] Copyright Office, *Frequently Asked Questions About the Section 1201 Rulemaking* (28 October 2018), online: Government of the United States of America <https://www.copyright.gov/1201/2018/faqs.html>.

independent repairers from providing services can lead to less choice for consumers and potentially higher prices. Moreover, IoT interoperability could be better understood with the help of a technical analysis on IoT and data protocols by software engineers and IT specialists. Finally, the important market influence of Internet giants suggests market research and economics analysis of IoT and data markets, including interviews with Canadian companies, could provide insights on the state of competition and innovation.

Appendix A — References for products documentation

Table A1— Documentation references

Products	EULA URL	Privacy Policy URL
Tesla Autopilot	https://www.tesla.-com/about/legal	https://www.tesla.-com/about/legal/le-gal#privacy-policy
NissanConnect	https://www.nis-san.ca/content/ dam/nissan/ca/ owners/nissancon-nect/pdf/nissancon-nectappstermsand-conditionsen-glish.pdf	https://s3-us-west2.a-mazonaws.com/ sxmcwv-nissandocs/ privacy_policy_-caen.pdf
FCA Uconnect	https://www.dri-veuconnect.ca/en/ sirius-xm-guar-dian-terms	https://www.driveu-connect.ca/en/sirius-xm-guardian-terms
Fitbit Charge 3	https://www.fitbit.-com/en-ca/legal/ terms-of-service	https://fitbit.com/en-ca/legal/privacy-pol-icy
Apple Watch Series 4	https://apple.com/ ca/legal/sla/ >	https://www.apple.-com/ca/legal/privacy/ en-ww/ >
Samsung Galaxy Watch	https://www.sam-sung.com/us/legal/ samsunglegal-eula-gear/	https://account.sam-sung.com/member-ship/terms/privacy-policy
North Focals	https://www.by-north.com/legal/ terms-and-condi-tions	https://www.by-north.com/legal/ tprivacy-policy
Oculus Go	https://www.ocu-lus.com/legal/ terms-of-service	https://www.oculus.-com/legal/privacy-policy/
Nest learning thermostat	https://nest.com/ ca/legal/eula/	https://nest.com/ca/ legal/privacy-state-ment-for-nest-pro-ducts-and-services/

Philips Hue Bulb	https://www2.meethue.com/en-us/product-terms?origin=15_global_en_applink_hueapp_productterms	https://2www2.meethue.com/en-gb/support/privacy-policy?origin=15_global_en_applink_hueapp_privacy
August Home Smart Lock Pro	https://august.com/pages/end-user-agreement	https://august.com/pages/privacy-policy
Arlo Pro 2	https://www.arlo.com/en-us/about/terms-and-conditions	https://www.arlo.com/en-us/about/privacy-policy
iRobot Roomba i7 +	https://webapi.irobot.com/Legal/Documents/North-America/Canada/Legal-Documents/EULA.aspx?sc_lang=en&_g-a=2.129427724.1428223747.1553545287-1005143356.1553545287	https://webapi.irobot.com/Legal/Documents/North-America/Canada/Legal-Documents/EULA.aspx?sc_lang=en&_g-a=2.129427724.1428223747.1553545287-1005143356.1553545287
Samsung Family Hub	https://www.samsung.com/us/commonsoftware_eula.html	https://account.samsung.com/membership/terms/privacypolicy
Sony Bravia TV	https://sony.com/electronics/support/res/manuals/4489/44890071m.pdf	https://products.sel.sony.com/sel/legal/privacy.html
Google Assistant	https://policies.google.com/terms	https://policies.google.com/terms?
Amazon Alexa	https://www.amazon.com/gp/help/customer/dis-	https://www.amazon.ca/gp/help/customer/display.html?no-

	play.html?nodeId = 201809740	deId = 201909010
Apple Siri	https://www.apple.com/legal/sala/docs/homepod.pdf	https://www.apple.com/legal/privacy/en-ww/ >
Samsung Bixby	https://www.samsung.com/us/legal/samsunglegal/-eula4/	https://www.samsung.com/us/account/privacy-policy
Amazon AWS IoT Button	https://aws.amazon.com/iot/button/terms	https://aws.amazon.com/privacy/

Appendix B — Case study questions

Study of business models

Does the seller propose an ownership model or a subscription model?
Can third parties control the device?
Can the user add applications from third-parties?
Are software or security updates available?
Are there costs associated with software/security updates?
Are repairs available only from authorized service providers?
Are there technical measures to secure the data?
Are there technological protection measures to restrict access to software integrated in the product?
Do suppliers explain whether they will use consumer usage data? If so, how they will use it?
Is the user invited to consent to his data being used?
Can the user access its data? If so, how?
Are there any major business models adopted by suppliers?
What are the main characteristics of the business models adopted with regard to the integrated software?

Study of end-user licenses

Are there limitations, restrictions, conditions, and other copyright terms imposed on consumers who purchase the product? If yes, what are they?

- Restrictions on resale or renting?
- Restrictions on the owner's ability to repair, modify, or refurbish the product?
- If yes, can the user modify, repair, or refurbish the product themselves?
- If yes, can the user use a separate device to circumvent any technological protection measures on the product to repair, modify, or refurbish it?
- If yes, can the user ask a third party repair shop to repair, modify, or refurbish the product?
- Are there restrictions on interoperability with other devices?
- Are there restrictions on the use of assistive technologies for persons with disabilities?
- Are there restrictions on access to an individual's personal information?
- Can any third party repair, modify, or refurbish the product?
- Are there disclaimers of limited liability for product defects, including software malfunction?