Canadian Journal of Law and Technology

Volume 15 | Number 1 Article 10

1-1-2017

A Whole New Meaning to Having Our Head in the Clouds: Voice Recognition Technology, the Transmission of our Oral Communications to the Cloud and the Ability of Canadian Law to Protect Us from the Dangers it Presents

Sarit K. Mizrahi

A Whole New Meaning to Having Our Head in the Clouds: Voice Recognition Technology, the Transmission of our Oral Communications to the Cloud and the Ability of Canadian Law to Protect Us From the Dangers it Presents

Sarit K. Mizrahi*

Abstract

Voice recognition technology is now included in modern devices as a matter of course, being used in anything from our cellular telephones, to our televisions, and even the toys of our children. While we may voluntarily interact with some of our devices using this technology, such as conversing with Siri on our iPhones, many of us remain unaware as to the dangerous implications of using voice recognition technology.

Its ability to record some of our most personal conversations allows private companies to eavesdrop on us in an unprecedented manner and amass highly sensitive information about our lives that would have previously been impossible. What is further pressing about this situation is that all of these recordings of our oral communications are stored in the cloud by these entities for future use and consultation, and are sometimes even transmitted to third parties. This risks exposing what may be some of our most intimate moments. Imagine if a commercial were targeted to a person's television based on a sensitive conversation they had in the privacy of their own home. Or, even more frightening, consider if a child predator were to communicate with a child through their Barbie doll and use this connection to discover their whereabouts.

The levels of security and privacy available through this use of voice recognition technology are therefore questionable, and the ability of Canadian law to adequately protect us in both these arenas is even more so. I seek to examine the inherent dangers that voice recognition technology presents to its users and whether the law properly addresses each of these risks. I will begin my analysis by exploring the security and privacy infrastructures employed by some of the foremost companies offering this technology, in an effort to determine if they are sufficiently robust to protect our private information. I will then turn my analysis to an in-depth examination of Canadian privacy laws so as to ascertain whether or not they are extensive enough to safeguard us from the numerous threats posed by this technology, to both our citizens in general and our children in particular.

---

* LL.B., J.D., LL.M. (Information Technology Law), University of Montreal; Ph.D. Candidate (Law and Technology), University of Ottawa; member of the Barreau du Québec.

INTRODUCTION

In this modern age, not only are our lives becoming significantly more interconnected,[1] but everything from our cell phones, to our TVs and even our children's toys are increasingly being equipped with voice recognition technology. Although we may voluntarily interact with some of our devices using this feature, many of us remain unaware as to its dangerous implications. Its ability to record our most personal conversations allows private companies to eavesdrop on us in an unprecedented manner[2] and ultimately use this biometric data to identify us, anywhere and at any time, through the unique sound waves we create.[3] What is further pressing about this situation is that *all* of these recordings are stored in the cloud,[4] whose security is difficult to guarantee,[5] which risks exposing what may be some of our most intimate moments.

In order to demonstrate the privacy and security risks involved with the use of voice recognition enabled devices, this article will concentrate on two such devices that epitomize these inherent dangers. The first is Samsung's Smart TV, which allows its users to control their televisions through voice commands while storing recordings of these interactions in the cloud. With its initial privacy policy implying that all spoken communications made in close proximity to the television would be captured,[6] this device illustrates how individuals may not

---

1 Last year there were 10 billion interconnected devices and it is expected to reach 34 billion by the year 2020. See Jonathan Camhi, "BI Intelligence Projects 34 Billion Devices Will Be Connected By 2020", *Business Insider* (6 November 2015), online: < www.businessinsider.com > .

2 David Talbot, "The Era of Ubiquitous Listening Dawns", *MIT Technology Review* (8 August 2013), online: < www.technologyreview.com > ; Stacey Gray, "Always On: Privacy Implications of Microphone-Enabled Devices", *Future of Privacy Forum* (April 2016), online: < www.fpf.org > ; Kayleen Manwaring, "A Legal Analysis of Socio-Technological Change Arising Out of eObjects" (5 January 2015) at 11, online: < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2690024 > ; Omer Tene & Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms" (2013) 16: 1 Yale JL & Tech 59; Ira S. Rubinstein, "Big Data: The End of Privacy or a New Beginning?" (2012) 3 Intl Data Priv L 74.

3 Elizabeth M. Walker, "Biometric Boom: How the Private Sector Commodifies Human Characteristics" (2015) 25:3 Fordham Intell. Prop Media & Ent LJ 831 at 840, 850; Anne T. McKenna, "Pass Parallel Privacy Standards or Privacy Perishes" (2013) 65:4 Rutgers LR 1041 at 1067; Joe Newman & Joseph Jerome, "'Press Start to Track?' Privacy and the New Questions Posed by Modern Videogame Technology" (2014) 42:4 AIPLA 527.

4 Lon A. Berk, "After *Jones*, the Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud" (2014) 14:1 J. High Tech LJ 1 at 4-8; Jenna Mäkinen, "Data Quality, Sensitive Data and Joint Controllership as Examples of Grey Areas in the Existing Data Protection Framework for the Internet of Things" (2015) 24:3 Inf & Comm Tech L 262 at 274.

5 See Nancy J. King & V. T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud" (2012) 28 Computer L & Sec Report 308.

6 This clause was, however, modified after having been the subject of much criticism last year. See Parmy Olson, "Samsung's Smart TVs Share Living Room Conversations With

even be at liberty to speak freely in their own homes without fearing the proverbial "Big Brother".

The second device that will be examined is Mattel's Hello Barbie, which is a WiFi enabled interactive doll that records a child's interactions through a microphone, processes this data in the cloud, and then uses it to have two-way conversations with the child.[7] By becoming a child's trusted friend, this doll is a prime illustration of technology that is geared to children and embodies the privacy and security risks that our youth faces in this modern age.[8] Consider, for example, the frightening possibility of a child predator communicating with a child through their Barbie and using this connection to gain their trust and discover their whereabouts.

Due to the fact that the voice recordings captured through such devices *allow for the possibility* of positively identifying their users,[9] any private company that collects and stores this data will have to abide by Canadian privacy laws.[10]

Third Parties" *Forbes* (9 February 2015), online: < www.forbes.com > ; Mäkinen, *supra* note 4 at 274; Susan Landau, "What Was Samsung Thinking?", *IEEE Computer and Reliability Societies* (May-June 2015) 3.

7 Matt Olsen, Bruce Schneier & Jonathan Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate", *Berkman Center for Internet & Society at Harvard University* (1 February 2016) at 14, online: ; Verónica Donoso et al., "Faraway, so close: why the digital industry needs scholars and the other way around" (2016) 10:2 J of Children & Media 200 at 200.

8 See Emmeline Taylor & Katina Michael, "Smart Toys that are the Stuff of Nightmares", *IEEE Technology and Society Magazine* (March 2016) 8; Meg Leta Jones & Kevin Meurer, "Can (and Should) Hello Barbie Keep a Secret?" (1 January 2016), online: < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2768507 > .

9 Although it is beyond the scope of this article, it is significant to note that the efficiency of such an expansive definition has been questioned since its inception and the constant evolution of technology has accentuated these doubts. See Éloïse Gratton, "If Personal Information is Privacy's Gatekeeper, Then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information" (2014) 24:1 Alb LJ Sci & Tech 105; Stephanie Perrin et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 54 ("The definition in the Act is limitless in terms of what can be information about an identifiable individual.").

10 With regards to the federal *Personal Information Protection and Electronic Documents Act*, RSC 2000, c 5 ["PIPEDA"], see *Gordon v Canada (Minister of Health)*, 2008 FC 258, 2008 CarswellNat 522. With regard to Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 ["ARPPIPS"], see *Antonio Sergi c Ville de Mont Royal*, [1977] CAI 198; *E c Office de la protection du consommateur*, [1987] CAI 350; *Ségal c Centre de services sociaux de Québec*, [1988] CAI 315. With respect to its application to modern technology, see Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001-25: A broadcaster accused of collecting personal information via Web site" (20 November 2001), online: < www.priv.gc.ca > ; Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-315: Web-centred company's safeguards and handling of access request and privacy complaint questioned" (9 August 2005), online: < www.priv.gc.ca > ; Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-319: ISP's anti-

Whereas most of Canada is governed by the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[11] Quebec is one of three provinces that enacted a substantially similar version of this law,[12] entitled the *Act Respecting the Protection of Privacy in the Private Sector* ("ARPPIPS"),[13] which takes precedence on its territory. Seeing as how the conference at which this article was presented took place in that province, the present privacy analysis will concentrate on both of these Acts.

Having been established over a decade ago, however, many have criticized the PIPEDA and the ARPPIPS as being inadequate to safeguard individual privacy. In addition to being afflicted with several loopholes that have not yet been addressed, constant advances in technology have significantly reduced the effectiveness of the protections provided.[14] This lack of efficiency is tremendously worrisome in light of the severe and unprecedented privacy violations that are enabled by devices equipped with speech recognition technology.

In this vein, this article will begin by (1) critically assessing the privacy policies governing both Samsung's Smart TV and Mattel's Hello Barbie in light of Canadian privacy laws so as to expose whether or not user privacy is effectively being protected. This analysis will then be followed by (2) a discussion of whether or not this state of affairs may be rectified by legislative interventions in light of other threats presented to users of interconnected devices.

---

spam measures questioned" (8 November 2005), online: < www.priv.gc.ca > ; Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2009-010: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection" (September 2009), online: < www.priv.gc.ca > (where IP addresses were considered as "personal data"); Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-13: Publisher collected and used e-mail addresses for marketing without consent" (2 June 2009), online: < www.priv.gc.ca > (where e-mail addresses were considered as "personal data"); *Finding #017: Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, 2013 CanLII 96099 (P.C.C.); Office of the Privacy Commissioner of Canada, "PIPEDA Report of Finding #2011-001: Google Inc. WiFi Data Collection" (20 May 2011) at para. 18, online: < www.priv.gc.ca > (where behavioural data was considered as "personal information").

11 PIPEDA, *ibid.*

12 The other two provinces are Alberta and British Columbia. See Office of the Privacy Commissioner of Canada, "Privacy Legislation in Canada" (May 2014), online: < www.priv.gc.ca > .

13 ARPPIPS, *supra* note 10.

14 See Office of the Privacy Commissioner of Canada, *The Case for Reforming the Personal Information Protection and Electronic Documents Act* (Ottawa: Office of the Privacy Commissioner of Canada, 2013) at 18, online: < www.priv.gc.ca > ; Éloïse Gratton, "Updating Quebec Private Sector Privacy Law — Part 2 of 2" (11 December 2015), online: *Éloïse Gratton* (blog) < www.eloisegratton.com > ; David Dubrovsky, "Protecting Online Privacy in the Private Sector: Is there a '*Better*' Model?" (2005) 18 RQDI 171 at 177.

I. THE CROSSROADS BETWEEN PRIVACY POLICIES GOVERNING VOICE RECOGNITION ENABLED DEVICES AND CANADIAN PRIVACY LAW: IS USER PRIVACY EFFECTIVELY BEING PROTECTED?

This part will examine the privacy policies of both Samsung's Smart TV and Mattel's Hello Barbie in light of the extent to which they adhere to Canadian privacy laws, as well as the manner in which gaps in the protection provided by these laws may aggravate the privacy violations that users of these devices could encounter. This analysis will concentrate on the principles of the PIPEDA and the ARPPIPS that are most relevant to the current discussion[15] and which oblige organizations to (1) identify the purposes for and impose limitations on the collection, use, disclosure and retention of personal data, (2) obtain meaningful or manifest consent, (3) safeguard the personal information collected, and (4) limit the cross-border transfer of this data.

(a) The Collection, Use, Disclosure and Retention of Personal Information: Identifying Purposes and Imposing Limitations

Both the PIPEDA and the ARPPIPS maintain that the purpose for the collection, use and disclosure of personal information must be both identified[16] and limited to that which is *relevant or necessary* to fulfill the purposes in question.[17] The PIPEDA further specifies that it must be restricted to what "a reasonable person would consider . . . appropriate in the circumstances."[18]

Samsung's Smart TV privacy policy appears to satisfy this requirement by specifying that they "collect [the user's] interactive voice commands only when [the user makes] a specific search request to the Smart TV by clicking the activation button ... and speaking into the microphone on the remote control."[19] While this button could be involuntarily pressed by Smart TV users, such that

---

[15] The other requirements are: accountability for and accuracy of the personal data under its control; openness about personal information handling practices; and providing individuals with both access to their personal data as well as the ability to challenge the organization's compliance to privacy laws.

[16] ARPPIPS, *supra* note 10, s. 5; PIPEDA, *supra* note 10, Schedule 1, s. 4.2.

[17] ARPPIPS, *supra* note 10, ss. 5, 12, 13; PIPEDA, *supra* note 10, Sch. 1, ss. 4.4, 4.5. See also Éloïse Gratton, "Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services" in *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels* (Cowansville: Éditions Yvon Blais, 2012) 7 at 17-20.

[18] PIPEDA, *supra* note 10, s. 3. See also Chris D. L. Hunt, "The Common Law's Hodgepodge Protection of Privacy" (2015) 66 UNBLJ 161 at 180; Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2005) 56:2 UTLJ 181 at 207-210 (explaining how this requirement is meant to better ensure fair information practices).

[19] Samsung, "Samsung Global Privacy Policy", at "Smart TV Supplement, Voice Recognition", online: < www.samsung.com/ca/info/privacy.html > .

their voice could be recorded against their will, this still provides them with as much control as possible over which audio is captured and thus appears appropriate under the circumstances. Moreover, particularly invasive uses of this biometric data are prevented by the fact that this personal information is only collected and used for the purposes of "[providing the user] with Voice Recognition features and [evaluating] and [improving] the features,"[20] rather than identifying them in public through the sound of their voice, for example.

Similarly to Samsung's Smart TV, the privacy policy applicable to Hello Barbie[21] specifies that they limit their collection to audio recordings of the voices captured when the button on Barbie's belt buckle is held down.[22] The possibility that undesired audio may be collected thus exists with this device as well. With the use of this data being significantly more extensive than that outlined by Samsung, however, this prospect is slightly more concerning. Essentially, they "use, store, process, convert, transcribe, analyze or review Recordings,"[23] and share them with their third party affiliates,[24] for the purposes of "[providing, maintaining, analyzing and improving] the functioning of the Services, [developing, testing or improving] speech recognition technology and artificial intelligence algorithms, or for other research and development and data analysis purposes"[25] as well as "providing quality control and . . . improving . . . the scripting of Hello Barbie."[26] With so many uses being made of this data, it is questionable as to whether or not a reasonable person would consider them appropriate.

Additionally, while both the privacy policies of Samsung's Smart TV and Hello Barbie specify that they share their customers' private data with their third party affiliates, the two companies differ significantly in the extent to which they allow their third party affiliates to use this information. For its part, Samsung's privacy policy specifies that they disclose the voice recordings they collect to a single third party, identified as being Nuance Communications, Inc., for the purposes of "[converting a user's] interactive voice commands to text . . . to the extent necessary to provide the Voice Recognitions features to [the user]."[27]

---

20 *Ibid.*

21 While Mattel's website contains a Hello Barbie privacy commitment, it is in fact ToyTalk's privacy policy that governs this doll, as they are the ones that manage the Barbie's speech recognition software.

22 Hello Barbie, "Privacy Commitment", online: < hellobarbiefaq.mattel.com/privacy-commitment > ; ToyTalk, "Hello Barbie Privacy Policy", at "What Information Do We Collect? Recordings", online: < www.toytalk.com/hellobarbie/privacy > .

23 ToyTalk, *ibid* at "What Information Do We Share With Third Parties?", "How Do We Use the Personal Information We Collect?".

24 ToyTalk, "Hello Barbie Companion Application Terms of Use", at "Speech Data, Recordings and Third Party Components", online: < www.toytalk.com/hellobarbie/terms > .

25 ToyTalk, *supra* note 22 at "How Do We Use the Personal Information We Collect?".

26 ToyTalk, *supra* note 24 at "Speech Data, Recordings and Third Party Components".

Though this does *technically* satisfy the requirement of limited disclosure, thus leading individuals to believe that Nuance Communications is the only third party company that has access to their personal information that is collected by Samsung, this is not actually the case.

Rather, Nuance Communications' own privacy policy maintains that the information given to them "shall only be used by Nuance or *[its associated] third parties* . . . to develop, tune, enhance, and improve Nuance services and products."[28] As this company does not specify which third parties act under its direction, it is impossible to consult the privacy policies of those entities. Suffice to say, this process can go on an infinite number of times, with each third party further disclosing voice recordings and other personal data to their own affiliates, who may use this biometric information for more privacy invasive purposes than the organization itself, such that there is very little *actual* limitation on the disclosure and ultimate use of that data.[29]

To this effect, it is often recommended for private corporations to contractually forbid their third party affiliates from re-transferring data, though this is rarely done as it is not a legal constraint.[30] That having been said, Hello Barbie's privacy policy is one of the few that has actually followed this suggestion by contractually prohibiting their third party affiliates from using the information disclosed to them for their own purposes.[31] Despite this, however, they do share some information with their affiliates, which they allow these entities to "use for their own research and development purposes, including developing, testing and improving speech recognition technology and artificial intelligence algorithms not related to the services or technology being provided."[32] While this use goes beyond what is strictly necessary to supply the initial service and thus runs afoul of both the PIPEDA and the ARPPIPS, it is significant to note that recordings of a child's voice are never shared thus at least preventing these third parties from making use of this sensitive biometric data for their own unknown purposes.

Finally, when it comes to limiting retention, Hello Barbie is submitted to more stringent requirements than Samsung because the former is geared towards children, whose personal information may not be collected or stored. They thus specify that they delete any such personal data that they become aware of and contractually compel their affiliates to do so as well.[33] Due to the fact that they

---

27 Samsung, *supra* note 19.

28 Nuance Communications, Inc., "Privacy Policy", at "Collected information and usage", online: < www.nuance.com > [emphasis added].

29 See Chris Matyszczyk, "Samsung Changes Smart TV Privacy Policy in Wake of Spying Fears", *CNet* (10 February 2015), online: < www.cnet.com > .

30 Gratton, *supra* note 17 at 20.

31 ToyTalk, *supra* note 22 at "What Information Do We Share With Third Parties?".

32 ToyTalk, *ibid.*

33 ToyTalk, *ibid* at "What Information Do We Collect? Recordings".

do not routinely monitor the children's recordings,[34] they place the responsibility of the children's safety on their parents who may access and delete all of their child's audio recordings should they wish. As it is unfeasible to screen all of these recordings for personal information, this approach appears balanced by ensuring the protection of the children's privacy whilst avoiding the violations associated with scanning all of this captured audio.[35]

Samsung's privacy policy, on the other hand, complies with this obligation simply by specifying that they retain their users' information only for as long as is necessary to fulfill the purpose for which it was collected.[36] Samsung's adherence to this provision is essentially rendered moot, however, because Nuance Communications' privacy policy does not denote anything regarding their retention of private data, thus providing very little limitation in this regard. Nevertheless, the problem here is not solely with Samsung, whose privacy policy technically respects the letter of both the PIPEDA and the ARPPIPS, but rather with the laws themselves, which do not efficiently protect the use, disclosure and retention of personal information.

(b) Meaningful or Manifest Consent

Both the PIPEDA and the ARPPIPS require that private companies that collect, use or disclose the personal information of their users must obtain their consent in a manner that is meaningful[37] or manifest, free and enlightened,[38] respectively. The approach taken to consent by both of these laws is, however, somewhat problematic. For its part, the PIPEDA maintains that consent will be meaningful as long as it is reasonable in light of the sensitivity of the information being collected.[39] Where the data in question *is* likely to be considered sensitive, as would be the case with audio captured through voice recognition devices, "[an] organization *should generally* seek express consent"[40] though they are not *necessarily obliged* to do so.

While this wisely leaves an opening for those circumstances under which obtaining express consent might not be feasible, it does very little to actually

---

[34] Mattel, "Hello Barbie Messaging/Q&A" (2015) at 4-5, online: <hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf>.

[35] ToyTalk, *supra* note 22 at "What Choices Do You Have Regarding the Use of Your Information?".

[36] Samsung, *supra* note 19 at "Data Retention".

[37] PIPEDA, *supra* note 10, Sch 1, s 4.3.2.

[38] ARPPIPS, *supra* note 10, s 14; it is also significant to note that Quebec's *Act to Establish a Legal Framework for Information Technology*, CQLR, c C-1.1 ["AELFIT"], states that biometric data may only be captured with express consent (*ibid*, s 44 at para. 1. See also E.M. Walker, *supra* note 3 at 861).

[39] PIPEDA, *supra* note 10, Sch 1, s 4.3.4. For an analysis of the issues involved with the PIPEDA's definition of what is reasonable in light of modern day technological advances, see Dubrovsky, *supra* note 14 at 177.

[40] PIPEDA, *supra* note 10, Sch 1, s 4.3.6 [emphasis added].

protect user privacy as it provides private corporations with a loophole that they often exploit to avoid acquiring the express consent of their customers even where it *is* possible.[41] By requiring that consent be "manifest," and thus explicit rather than implied, the ARPPIPS is more respectful of user privacy by preventing companies from bypassing this obligation, but it has proven difficult to adapt it to the new realities of our interconnected world.[42] As such, the consent provision of the PIPEDA is significantly easier for Web-based companies to adhere to than that of the ARPPIPS.

Although both Samsung's and Hello Barbie's privacy policies are sufficient to conform to the PIPEDA in this regard, only the latter complies with the ARPPIPS. Essentially, the data supplied by these companies about their information handling practices[43] arms people with the knowledge they need to meaningfully consent[44] for the purposes of the PIPEDA, such that it can be implied through their mere purchase of the devices in question.[45] This remains so even in the case of Samsung's privacy policy, which does not inform individuals about how their private information is being further used[46] by its third party affiliates,[47] even though it might be difficult to consider this form of consent as meaningful in the true sense of the word.[48] On the other hand, only Hello Barbie's policy complies with the ARPPIPS in this respect. Whereas Samsung's policy is silent on any additional measures taken to gain express consent, the Hello Barbie policy notes that parents are given the opportunity to manifestly demonstrate their consent by clicking a button[49] when they setup the online account required to activate the doll.[50]

---

41 For example, it would not be terribly difficult for voice recognition enabled devices to be equipped with a setup wizard that would allow for their users' express consent through the click of a button. See Office of the Privacy Commissioner of Canada, *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act* (Ottawa: Office of the Privacy Commissioner of Canada, 2016) at 13, online: < www.priv.gc.ca > .

42 Gratton, *supra* note 14; Éloïse Gratton, "Beyond Consent-Based Privacy Protection" (11 July 2016), online: *Éloïse Gratton* (blog) < www.eloisegratton.com > .

43 See *supra* notes 16 to 36 and accompanying text.

44 Office of the Privacy Commissioner of Canada, *supra* note 41 at 2-3.

45 Gratton, *supra* note 14.

46 Office of the Privacy Commissioner, *supra* note 41 at 6.

47 While this is not a legal requirement, the lack of transparency regarding the disclosure of personal information to third parties has been identified as a significant issue by the Privacy Commissioner of Canada (*ibid* at 12, 16).

48 Austin, *supra* note 18 at 188.

49 Gratton, *supra* note 14. See also Sarit K. Mizrahi, *The Legal Implications of Internet Marketing: Exploiting the Digital Marketplace Within the Boundaries of the Law* (Cowansville: Éditions Yvon Blais, 2015) at 90-94.

50 ToyTalk, *supra* note 22. See Jones & Meurer, *supra* note 8 at 2.

Despite the general adherence of these policies to the obligation to obtain user consent, it is important to note that the PIPEDA and the ARPPIPS maintain that meaningful or manifest consent loses its legitimacy when it is presented as a precondition to an individual's ability to enjoy goods or services.[51] Though this is meant to prevent companies from forcing individuals to agree to disclose their personal information solely so as not to be deprived of this benefit, it is difficult to reconcile this principle with the use of voice recognition enabled devices. Essentially, interacting through speech, and thus allowing voice recordings to be captured and stored in the cloud, is absolutely necessary in order to be able to use the products in question.[52]

This is likely the reason for which Hello Barbie's privacy policy does not address the possibility of refusing to allow the doll to capture voice recordings. Although not sufficient to satisfy the ARPPIPS, the simple act of purchasing the doll armed with the knowledge of how it functions should technically be enough to presume that people consent to this use. The same logic could not, however, apply to Samsung's Smart TV as the voice recognition ability is merely one feature of the device, which is otherwise similar to any television and can be used as such. To this extent, its privacy policy specifies that users may disable the voice recognition feature but that doing so would prevent them from controlling their TV through speech, except for certain predefined voice commands.[53] Even though refusing to agree to their voice recordings being captured prevents individuals from using the product to its fullest extent, Samsung's implementation of predefined voice commands that may still be used, despite this, is quite novel in the company's attempt to respect this requirement under the circumstances.

(c) Security Safeguards

Both the PIPEDA and its Quebec counterpart provide that the personal information collected must be protected using security measures that are reasonable in light of the sensitivity of the data in question.[54] While the PIPEDA specifies the measures that must be taken to this effect, it is rather Quebec's *Act to Establish a Legal Framework for Information Technology* ("AELFIT")[55] that outlines the safeguards that must be implemented for the purposes of the ARPPIPS. For its part, the PIPEDA maintains that such security measures must ensure that personal data is protected against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.[56] The AELFIT,

---

[51] ARPPIPS, *supra* note 10, s 9; PIPEDA, *supra* note 10, Sch 1, s 4.3.3.

[52] Office of the Privacy Commissioner of Canada, *Guidelines for Online Consent* (Fact Sheet) (Ottawa: Office of the Privacy Commissioner of Canada, 2013) at 4, online: < www.priv.gc.ca > .

[53] Samsung, *supra* note 19.

[54] ARPPIPS, *supra* note 10, s. 10; PIPEDA, *supra* note 10, Sch 1, s 4.7.

[55] AELFIT, *supra* note 38.

on the other hand, states that such data must be protected by technological means that prevent any alteration of the information whilst also protecting its confidentiality.[57] This must be achieved through the use of techniques such as access controls, which prevent unauthorized access to this data when it is at rest,[58] as well as through means appropriate to the mode of transmission, that protect it throughout its transfer.[59] Additionally, both laws require that contractual or other means must be used by the company to ensure that any data it transfers to a third party is assured a comparable level of protection.[60] This obligation is significant in that it could have far reaching positive effects by indirectly forcing these third party affiliates to impose similar responsibilities upon their own service providers with whom they might share this data, thus somewhat remedying the issues identified above surrounding the constant re-transfer of data between affiliates.[61]

While Samsung's and Hello Barbie's privacy policies outline the security safeguards instilled to protect personal information, the latter does so to a greater extent than the former. Samsung's policy merely includes a broad clause stating that it employs reasonable physical and technical measures to safeguard the personal information it collects.[62] For its part, the privacy policy applicable to Hello Barbie specifies that they "take reasonable measures to protect personal information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration, and destruction. For example, [they] use secure, encrypted communications when transferring all personal information over the web."[63] By being more detailed, not only does this clause cover all the provisions set forth by both federal and Quebec privacy laws, but it also assures its users that stringent security measures are implemented which truly take into account the highly sensitive nature of the biometric data collected by this doll.

Instituting security safeguards within their own organization, however, is only one part of the responsibility imposed on them in this respect. They are also obliged to ensure that the third parties to whom they disclose the personal information of their clients similarly protect it. With Hello Barbie's affiliates not being identified and its privacy policy not addressing this matter, it is impossible

---

56 PIPEDA, *supra* note 10, Sch 1, s 4.7.1.

57 AELFIT, *supra* note 38.

58 *Ibid*, s. 25.

59 *Ibid*, s. 34.

60 *Ibid*, s. 26; PIPEDA, *supra* note 10, Sch 1, s 4.1.3. For the interpretation of these requirements by Quebec courts, see *Deschesnes c Groupe Jean Coutu (PJC) inc.*, 2000 QCCAI 216, 2000 CarswellQue 3590, EYB 2000-178499 (CAI Qué); *Syndicat des employés de la ville de Huntington v Ville de Huntington*, AZ-97151510; *X v La Métropolitaine*, AZ-95151504.

61 See *supra* notes 27 to 30 and accompanying text.

62 Samsung, *supra* note 19 at "What do we do to keep your information secure?".

63 ToyTalk, *supra* note 22 at "What Steps Do We Take to Protect Your Information Online?".

to conclude as to their adherence to this requirement. Samsung, on the other hand, clearly does not satisfy this condition of both the PIPEDA and the ARPPIPS, as the privacy policy of its third party affiliate does not even mention the implementation of any security measures, but rather only states that they will notify their clients should a security breach occur.

(d) Limitation on the Cross-Border Transfer of Personal Information

Whereas the PIPEDA does not prohibit the transmission of personal information outside Canada,[64] the ARPPIPS forbids the transfer of this data across Quebec borders where it might be used for a purpose other than that which was identified.[65] If such a cross-border transfer is made, an organization will have to conclude a contract obliging the foreign third party to protect the data in question to the extent imposed by Quebec law.[66] Despite this, where the foreign jurisdiction's national laws would override this contract and permit unauthorized access to this data, such as the United States' PATRIOT Act,[67] it is questionable as to whether such a transfer would be possible. While the fact that the *legal risk* that this information will be accessed for national security purposes is comparable between both Canada and the United States and *may* thus be a sufficient basis upon which to enable personal data to be stored in the latter country,[68] this is not an established exception. Moreover, it is debatable as to whether this position would even be adopted in regards to biometric voice data, which is significantly more sensitive and privacy invasive than the personal information that has been available up to this point.

Though both Samsung's and Hello Barbie's privacy policies note that they may transfer the data and recordings that they collect to the United States as well as other unspecified countries,[69] they do not mention any additional measures taken to protect this transferred personal information to the degree required by the ARPPIPS. This does not, however, preclude them from complying with this

---

[64] The Office of the Privacy Commissioner of Canada has, however, issued guidelines to this effect. See Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Information Across Borders* (Ottawa: Office of the Privacy Commissioner of Canada, 2009), online: < www.priv.gc.ca > .

[65] ARPPIPS, *supra* note 10, s 17.

[66] Gratton, *supra* note 17 at 21.

[67] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, 115 Stat. 272 (2001).

[68] Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-313: Bank's notification to customers triggers PATRIOT Act concerns" (19 October 2005), online: < www.priv.gc.ca > ; Karl Delwaide, "Quebec Privacy Law Poses Difficulties for Outsourcing of Personal Information" (2007), 27 Lawyers Weekly 14; Nicolas W. Vermeys, Julie M. Gauthier & Sarit Mizrahi, "Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec", *Cyberjustice Laboratory* (10 July 2014) at 117, online: < www.cyberjustice.ca > .

[69] Samsung, *supra* note 19 at "Consent to International Transfer of Data"; ToyTalk, *supra* note 22 at "International Users".

condition, which maintains that cross-border transfers can occur as long as the individual consents to their private information being used for purposes not relevant to the ones identified.[70] Taking advantage of this exception, both Samsung and Hello Barbie impose this consent upon their users. Although this imposed consent may technically satisfy the non-transfer provision of the ARPPIPS, the fact that it strips users of their free choice in the matter violates this Act's prohibition against making consent a precondition to the ability to use the services unless it is necessary for the performance of the contract in question,[71] as discussed above.[72] In this light, it may be difficult to hold that these privacy policies satisfy the ARPPIPS' limitation on the cross-border transfer of personal data.

Between the privacy policies of Samsung's Smart TV and Mattel's Hello Barbie neglecting to adhere to certain provisions of federal and Quebec privacy laws, and those laws themselves being afflicted with gaps in privacy protection that are being taken advantage of by these companies, there is ultimately very little actual protection being afforded to voice recordings captured through speech recognition technology such that users of these devices are exposed to all the significant risks involved with their use. While legislative intervention might remedy these particular issues, the nature itself of such interconnected devices still presents certain hindrances to effective privacy protection that the enforcement of laws may not be able to remedy, as will be discussed in further detail in the next part.

II. CLOUDY SKIES AHEAD: WILL LEGISLATIVE INTERVENTION MAKE A DIFFERENCE IN LIGHT OF OTHER THREATS TO THE PRIVACY OF VOICE RECOGNITION DEVICE USERS?

Although the previous part of this article illustrates the inefficient privacy protections afforded by privacy policies and privacy laws alike, these faulty safeguards are not nearly as much of a threat to the protection of voice recognition enabled devices as hackers. The *raison d'être* of these individuals is to discover and exploit any security flaws they might find so as to gain access to the private information of individuals and ultimately use it for their own nefarious purposes.[73] With the number of interconnected devices exponentially increasing over time, malicious users further enjoy an abundance of attack vectors from which to choose.[74]

---

[70] ARPPIPS, *supra* note 10, s 17(1).

[71] ARPPIPS, *supra* note 10, s 9.

[72] See *supra* notes 51 and 52 and accompanying text.

[73] See Bryan Borzykowski, "The Chilling Truth about Cybercriminals — From a Paid Hacker", *CNBC* (26 July 2016), online: < www.cnbc.com > .

[74] See Office of the Privacy Commissioner of Canada, *The Internet of Things: An Introduction to Privacy Issues With a Focus on the Retail and Home Environments* (Ottawa: Office of the Privacy Commissioner of Canada, 2016) at 21-22, online:

Both Smart TVs as well as Hello Barbie have been hacked on numerous occasions. Malicious users have installed malware on Smart TVs, which not only gave them access to all the personal data that was aggregated by the television and stored in the cloud, but also allowed them to manipulate the TV's software and force a ransom to be paid in order to free the system.[75] The ability for hackers to overtake the television's system has further rendered it possible for these individuals to record and access *everything* an individual says in the vicinity of the device in question.[76] Thus, even though the companies providing voice recognition services through televisions may assure their users that their devices do not collect all their oral communications, such a serious violation of privacy still remains a possibility.

Hello Barbie has, however, been even further afflicted with security vulnerabilities since its release into the market.[77] One security flaw discovered allowed hackers to break the doll's encryption and access the voice recordings of the children that had been stored on remote cloud servers.[78] Another system weakness rendered it possible to access the personal accounts of Hello Barbie users by attempting to guess their passwords an unlimited number of times without being locked out of the system.[79] Yet neither of these examples is quite as

---

< www.priv.gc.ca > ; Office of the Privacy Commissioner, *Privacy and Cyber Security: Emphasizing Privacy Protection in Cyber Security Activities* (Ottawa: Office of the Privacy Commissioner of Canada, 2014) at 1, online: < www.priv.gc.ca > ; Borzykowski, *ibid.*

75 Mary-Ann Russon, "It's Official, Your Smart TV Can be Hijacked: Malware is Holding Viewers to Ransom", *International Business Times* (12 January 2016), online: < www.ibtimes.co.uk > . See also Benjamin Michéle & Andrew Karpow, "Demo; Using Malicious Media Files to Compromise the Security and Privacy of Smart TVs" (Paper delivered at the IEEE 11th Consumer Communications and Networking Conference, Las Vegas, 10 January 2014) in *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (Las Vegas: IEEE, 2014) 1144 (which describes a method of attack that would allow hackers to gain complete and permanent control over a Smart TV). For a discussion regarding how this is becoming problematic with respect to many interconnected devices, see: David Booth, "Ransomware: The Future of Car Theft?", *Montreal Gazette* (25 April 2016), online: < www.pressreader.com > ; "University of Calgary paid $20K in ransomware attack", *CBC News* (7 June 2016), online: < www.cbc.ca > .

76 Jacob Kittilstad, "Smart TVs Voice Recognition Software Could be Vulnerable to Hackers", *WDJT Milwaukee* (9 February 2016), online: < www.cbs58.com > ; Vijay Prabhu, "Hackers can spy on what you say by hacking Sony made Android TVs", *Techworm* (27 May 2016), online: < www.techworm.net > .

77 See "Hello Barbie App, Hello Security Issues: Security Risks Discovered with Mattel Hello Barbie Demonstrates Internet of Things Security Concerns", *Bluebox* (12 April 2015), online: < www.bluebox.com > .

78 Richard Adhikari, "Hello Barbie, Can We Talk About Your Security Issues?", *Tech News World* (8 December 2015), online: < www.technewsworld.com > .

79 Matthew Braga, "More Security Vulnerabilities Found in Hello Barbie Toy's Servers", *Motherboard* (25 January 2016), online: < motherboard.vice.com > .

disconcerting as when a security researcher was able to entirely take over the Hello Barbie doll *without much effort* and not only garner access to all the children's voice recordings captured by the doll and stored in the cloud, but also alter all of the doll's pre-recorded responses, thus allowing unauthorized third parties to communicate with the children and potentially expose them to inappropriate content.[80]

In light of these risks, the question at this juncture is thus whether or not more robust privacy legislation would better protect the captured voice recordings of this country's citizens, and perhaps prevent these types of severe violations. Though many consider that Canadian privacy law no longer responds to the needs of our interconnected society,[81] we are not convinced that legislative intervention would be terribly effective towards preventing hackers from taking advantage of security vulnerabilities. That having been said, we will address some potential changes that we believe would better protect the privacy of Canadians from private companies by remedying the issues exposed in the previous part of this article.[82]

To begin with, we propose that the obligation to limit the disclosure of the personal information aggregated be further extended to compel organizations to contractually prohibit their third party affiliates from making any further use of that data for their own purposes. This would, to a certain extent,[83] prevent the continuous re-transfer of data between partners and affiliates such that the private information of individuals would be used *strictly* for the purposes of providing them with the services to which they ascribed and nothing more.[84]

Moreover, in addition to obliging companies to contractually necessitate that their affiliates properly ensure the security of the personal data disclosed to them, it might be wise to compel organizations to include a clause that would allow them "a right of oversight, monitoring, and [a] right to perform an audit of the services being provided by the partners and the premises of the partners to ensure that they are acting in compliance with relevant Canadian data protection laws."[85] Not only would this be beneficial to consumers, as it would serve to

---

[80] Adhikari, *supra* note 78; Samuel Gibbs, "Hackers can hijack Wi-Fi Hello Barbie to Spy on Your Children", *The Guardian* (26 November 2015), online: < www.theguardian.-com > .

[81] See Office of the Privacy Commissioner of Canada, *supra* note 14.

[82] An in-depth discussion of all the legislative changes that may be necessary is beyond the scope of this article. For suggestions to this effect that were presented at the conference at which this article was delivered, see Avner Levin's article in this issue. See also Office of the Privacy Commissioner of Canada, *ibid* at 5-10; Dubrovsky, *supra* note 14 at 180.

[83] Essentially, where such a transfer is necessary for the purposes of providing the service, it will occur either way.

[84] Office of the Privacy Commissioner of Canada, *supra* note 41 at 16.

[85] Gratton, *supra* note 17 at 28 (while companies must contractually oblige their third party affiliates to respect Canadian privacy laws, this obligation does not go as far as requiring them to supervise these entities).

better ensure that the security of their personal information is being adequately protected, but it will likely be favourable to private companies as well, because they may ultimately be held responsible for any security breaches suffered by their partners and it is thus in their best interests to prevent such an event inasmuch as possible.[86]

Additionally, we would suggest that companies be compelled to specifically identify any third party affiliates with whom they share the personal data they aggregate. Although this was recommended in early case law following the adoption of the PIPEDA,[87] neither that Act nor the ARPPIPS impose it as a requirement. With individuals being unlikely to take the additional step of consulting the privacy policies of these third parties, however, we would further propose that companies be obliged to include the clauses of their affiliates that may affect the ultimate protection of the private data that is shared with these entities. Though this may lengthen privacy policies, thus going against the industry's attempts to simplify these documents, it is important to ensure that individuals are armed with this information so that they may be as well-informed as possible regarding how their personal information is being handled.[88]

Finally, in order to remedy those situations in which the law *does* foresee certain privacy protections that organizations neglect to adhere to, we would propose that the current privacy enforcement mechanism be strengthened in two ways. Firstly, we would suggest increasing the powers afforded to the Privacy Commissioner of Canada ("PCC"), as has often been recommended.[89] Essentially, while the ARPPIPS provides Quebec's *Commission d'accès à l'information* with the power to impose orders on companies that do not comply with this Act,[90] the PIPEDA does not endow the PCC with any direct enforcement powers,[91] which presents an enormous obstacle to this Act's efficiency as well as to the mission of the PCC. Secondly, we would propose to follow Quebec's example by providing citizens with the ability to sue companies in civil liability or tort for privacy violations[92] — a general right that is not

---

86 See also Gratton, *ibid.*

87 John Lawford, "Consumer Privacy Under *PIPEDA*: How Are We Doing?", *Public Interest Advisory Centre* (November 2004) at 51, online: < www.piac.ca > .

88 This would make people aware of the possibility that an organization's affiliates do not handle personal information similarly to the company itself, but rather use it for other purposes (see *supra* notes 27 to 32 and accompanying text).

89 See Office of the Privacy Commissioner of Canada, *supra* note 14 at 5-10; Lisa M. Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (2006) 44:1 Can Bus L.J. 21; Jennifer Stoddart, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA" (2006) 44:1 Can Bus LJ 1; Dubrovsky, *supra* note 14 at 180-181.

90 ARPPIPS, *supra* note 10, s 55.

91 PIPEDA, *supra* note 10, s 12.1(1).

92 Quebec's Civil Code allows for civil pursuit the moment someone has violated the law, such as the ARPPIPS, in a manner that caused damages to another (*Civil Code of Quebec*,

bestowed upon all Canadians.[93] In effect, the fear of such pursuit may provide companies with an additional incentive to respect privacy laws to the highest extent possible.

Although these suggested legislative modifications may better safeguard the personal data of individuals from private companies, they will not be terribly effective at protecting the privacy of individuals from hackers who will discover and exploit security weaknesses to gain access to this information. Requiring that more stringent security measures be instituted by companies would not prevent this probability, as any interconnected device will inevitably suffer from security flaws that will be taken advantage of by malicious users.[94] With these individuals using the internet to remain anonymous, it becomes virtually impossible to discover their identities and hold them accountable for their actions.[95] Although the regulation of hackers may be a hopeless endeavour, the ability of these recommended legislative changes to more efficiently regulate the protection of private information by corporations is certainly a step in the right direction.

III. CONCLUSION

As is exposed throughout this article, Canada's privacy laws are not sufficiently robust to adequately safeguard its citizens' personal information collected via voice-recognition enabled devices. Additionally, the fact that private companies often neglect to adhere to the provisions of these laws not only further deprives Canadians of whatever protection is afforded to their personal data, but it also places them at the mercy of unscrupulous hackers.

While this article limits itself to demonstrating the privacy breaches suffered by users of speech-recognition enabled devices at the hands of both private corporations and hackers, it is important to note that these entities are not the

---

SQ 1991, c 64, art 1457). For a more extensive discussion regarding the manner in which this might extend to pursuits for privacy violations, see Mizrahi, *supra* note 49 at 67-117.

93 In addition to Quebec, only British Columbia, Manitoba, Saskatchewan and Newfoundland have statutory torts of invasion of privacy, with Ontario being the only province with a common law tort to this effect. For a more in-depth discussion regarding the limited ability of Canadians to sue for privacy violations, see Hunt, *supra* note 18.

94 Glenn A. Fink et al., "Security and Privacy Grand Challenges for the Internet of Things" (Paper delivered at the International Conference on Collaboration Technologies and Systems, Atlanta, 1 June 2015) in *2015 International Conference on Collaboration Technologies and Systems (CTS)* (Atlanta: IEEE, 2015) 27 at 30-31; Office of the Privacy Commissioner of Canada, *Privacy and Cyber Security*, *supra* note 74 at 2-5.

95 Although this is considered as an indictable offense by the *Criminal Code of Canada*, RSC 1985, c. C-46, s. 184. See also Borzykowski, *supra* note 73; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. (Maryland: Elsevier, 2011) at 691-699; Kenneth Geers, "The Challenge of Cyber Attack Deterrence" (2010) 26:3 Computer L & Sec Report 298; H. L. Armstrong & P. J. Forde, "Internet Anonymity Practices in Computer Crime" (2003) 11:5 Inform Mgmt & Comp Sec 209; Dave Seglines & Lynn Burgess, "Canada 'failing' in fight against cybercrime, hacking", *CBC News* (24 November 2015), online: < www.cbc.ca > .

only ones that might risk invading the privacy of individuals by accessing the voice recordings captured by such devices. Law enforcement has also taken a significant interest in these voice captions in the hopes that they might prove useful in solving criminal investigations. In a recent case involving the Amazon Echo — a voice controlled personal assistant meant to turn houses into "smart homes"[96] — police in Benton County, Arkansas attempted to compel Amazon to turn over the voice recordings captured by the Echo device that was used in a murder suspect's home.[97] Although Amazon refused to provide anything other than account details in response to the warrant issued, such refusal has not always stopped law enforcement from performing searches within the cloud where these snippets of voice recordings are stored.[98] In addition to these searches enabling police to acquire cloud data attributed to criminal suspects, they also leave innocent cloud users vulnerable to the risk of having their data incidentally accessed as a result of the lack of segregation between the information of public cloud users.[99] As such, the privacy violations to which users of voice-recognition enabled devices may be subjected go well beyond the substantial ones that have already been exposed throughout this article.

Although some legislative changes may serve to better preserve the privacy of Canadians using such devices, there is no law that will alter the privacy and security threats that are heightened through the use of interconnected modern technology. Their ability to capture details about the habits and biometrics of individuals and store them in remote cloud servers, whose security is not guaranteed, leaves users with only two real options when it comes to their privacy: either accept the risks involved or modify their use of these devices accordingly.

---

96 TNI Editorial Team, "Amazon Echo: Complete and Detailed Review", *TNI* (8 January 2017), online: < www.technewsinc.com > .

97 Gary Robbins, "Murder Case Will Test Privacy Rights of Amazon Echo Users", *The San Diego Union-Tribune* (3 January 2017), online: < www.sandiegouniontribune.-com > ; Mike Juang, "Servant or Spy? Law enforcement, privacy advocates grapple with brave new world of AI assistants", *CNBC* (8 January 2017), online: < www.cnbc.com > .

98 See Sarit K. Mizrahi, "The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users During the Course of Criminal Investigations in Canada and the United States" 25 Tul J Intl & Comp L [forthcoming in 2017].

99 *Ibid.*