Université de Montréal

The Right to Privacy through the Development of Smart Technologies: How our Personal Health Data is Affected

Par

Yuliia Zhezherun

Faculté de droit

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de maîtrise en droit (LL.M.)

option droit international

septembre 2020

Université de Montréal

Faculté des études supérieures et postdoctorales

Ce mémoire intitulé :

The Right to Privacy through the Development of Smart Technologies: How our Personal Health Data is Affected

Présenté par

Yuliia Zhezherun

A été évalué(e) par un jury composé des personnes suivantes

Nicolas Vermeys
Directeur de recherche

Catherine Régis
Codirecteur

Vincent Gautrais
Membre du jury

Pierre Trudel
Membre du jury

Résumé

L'évolution de la technologie, nonobstant ses apports, peut enfreindre certains de nos droits fondamentaux puisqu'elle se développe plus rapidement que ces derniers. Ce mémoire vise à relever les défis que les technologies intelligentes peuvent poser tant sur la santé des communautés que sur les droits fondamentaux. La thèse porte sur les contraintes juridiques, présentes et à venir, notamment sur le droit à la vie privée à travers le développement et l'usage des technologies intelligentes qui captent notre information personnelle en lien avec la santé. Plus précisément, ce travail analyse si les bénéfices de l'accès à notre information à travers les technologies intelligentes en vue d'améliorer la santé et la sécurité des populations surpassent les conséquences juridiques.

Ce travail explore, entre autres, le potentiel des technologies intelligentes, leurs avantages individuels et collectifs, notamment en matière de santé publique, et les violations des droits de l'Homme que leur usage peut générer. Mais encore, il présente des innovations technologiques qui permettent d'améliorer les systèmes de santé étatiques afin d'être en mesure de mieux réagir aux futures épidémies, notamment au niveau international, comme à l'OMS. Ces données, suivies des autres complications possibles du fait d'un usage accru des technologies intelligentes qui restreignent notre vie privée, permettront de conclure si une telle intrusion peut être justifiée dans une société libre et démocratique.

Finalement, ce travail regarde les limites de l'acceptabilité sociale de l'intrusion dans la vie privée en échange à de meilleures conditions de santé afin que les organes étatiques et supra-étatiques puissent prendre des décisions éclairées, sans que les droits constitutionnels soient violés. Ce travail permettra de comprendre les enjeux que notre système judiciaire inévitablement devra surmonter en proposant des stratégies visant la prévention des maladies et autres problèmes de santé à travers l'usage des technologies intelligentes. Une des solutions principales proposées est la création de bases de données nationale et internationale à l'OMS qui captent les données des appareils intelligents portables.

Mots-clés : droits et libertés, technologies de l'information, appareils intelligents portables, intelligence artificielle, COVID-19, vie privée, santé et sécurité.

Abstract

The evolution of technology, notwithstanding its benefits, can negatively impact some of our fundamental rights as it develops faster than the latter. Indeed, this thesis aims to meet challenges generated by smart technologies and the impact they can have on the health of communities as well as on our fundamental rights. This thesis focuses on the legal constraints, present and to come, including the right to privacy, through the development and use of smart technologies that seize our personal health information. More specifically, this work seeks to analyze whether the benefits of accessing our information through smart technologies to improve the health and safety of populations outweigh the legal consequences.

This work explores the potential of smart technologies, the interest in using them individually and collectively, especially in the public health sector, and the human rights violations their use can generate. Moreover, it looks at technological innovations that help improve State health systems to be able to better respond to future epidemics, particularly at the international level, such as at the WHO. These data, followed by other possible complications due to the increased use of intelligent technologies that restrict our privacy, will allow us to conclude whether such an intrusion in our right to privacy can be justified in a free and democratic society.

Finally, this work examines the limits of the social acceptability of the invasion of privacy in exchange for better health conditions so that States and supra-State bodies can make informed decisions, without violating constitutional rights. This work will help us understand the issues that our judicial system will inevitably face while proposing strategies for the prevention of diseases and other health problems through the use of smart technologies. One of the main proposed solutions is the creation of a national and international database at the WHO generated by the data of smart health devices.

Keywords: rights and freedoms, information technology, smart wearable devices, artificial intelligence, COVID-19, right to privacy, health and safety.

Table of Contents

LIST OF ACRONYMS AND ABBREVIATIONS

AF: Atrial fibrillation

AI: Artificial intelligence

Alta L. Rev: Alberta Law Review

BC WCAT: Workers' Compensation Appeal Tribunal

BFOR: Bona fide occupational requirement

Cal. L. R.: California Law Review

CCQ : Civil Code of Quebec

CHA: Canada Health Act

CUSMA: Canada-United States-Mexico Agreement

Digital Evidence & Elec. Signature L Rev: Digital Evidence and Electronic Signature Law Review

EU: European Union

F.C.: Canada Federal Court Reports

F.C.A.: Federal Court of Appeal

FLIR: Forward Looking Infra-Red

GDP: Gross Domestic Product

GDPR: General Data Protection Regulations

GHO: Global Health Observatory

GPHIN: Global Public Health Intelligence Network

Healthc Inform Res: Journal of Healthcare Informatics Research

HER: Electronic Health Record

HIA: Alberta's Health Information Act

HR : Heart Rate

ILI: Influenza-like illness

IMF: International Monetary Fund

Int Neurourol J: International Neurourology Journal

Int. J. Commun. Syst: International Journal of Communication Systems

Int. J. Med. Inform.: International Journal of Medical Informatics

IoT: Internet of Things

ISO: International Standards Organization

J Ind Inf Integr: Journal of Industrial Information Integration

NAFTA: North American Free Trade Agreement

NSCA: Nova Scotia Court of Appeal

OAS: Organization of American States

OPC: Office of the Privacy Commissioner of Canada

PHI: Personal health information

Philos Trans R Soc Lond B Biol Sci.: Philosophical Transactions of the Royal Society of London

PHM: Population health management

PII: Personally identifiable information

PIPEDA: Personal Information Protection and Electronic Documents Act

PLoS Comput Biol: PLOS Computational Biology

Proc Natl Acad Sci USA: Proceedings of the National Academy of Sciences of the United States of America

QCCA : Court of Appeal

QCCLP: Commission des lésions professionnelles du Québec

QCCS : Cour supérieure du Québec/Quebec Superior Court

QCTDP: Human Rights Tribunal

R. du B.: Revue du Barreau du Québec

R.J.Q.: Recueil de jurisprudence du Québec

R.S.C. : Revised Statutes of Canada

RBT: Remote Biosensing Technologies

REM: Rapid Eye Movement

RLRQ: Recueil des lois et des règlements du Québec

RTNU: Recueil des Traités des Nations Unies

S.C.R.: Supreme Court Reports

SARS: Severe Acute Respiratory Syndrome

SCC: Supreme Court of Canada

SSN: Social Security Number

Stellenbosch L. Rev: Stellenbosch Law Review

U.N.B.L.J.: University of New Brunswick Law Journal

UNTS: United Nations Treaty Series

UOLTJ: University of Ottawa Law and Technology Journal

USMCA: United States–Mexico–Canada Agreement

WHO: World Health Organization

I would like to dedicate this to my parents without whom this opportunity would not have been possible; to my best friends and my partner for supporting me through it all; and to my professors who gave me confidence, strength and the will to pursue graduate studies while pushing my limits; but mostly, I would like to thank everyone who believed in me, even when I doubted myself.

ACKNOWLEDGMENTS

I would like to give my utmost gratitude to my two thesis directors, Nicolas Vermeys and Catherine Régis, who have allowed me to follow two of my biggest passions: public health and law, while combining them into one thesis. I am forever grateful for your time and your guidance. I thank you for supporting me throughout this journey, for being patient and available, for being incredible mentors, and for pushing me beyond what I thought I could achieve.

Introduction

Can anyone truly expect privacy in an era where humans are now dependent on technology? While some technologies are luxuries in our own homes[1], others are seen as necessities. In either case, there is perhaps something to be concerned about regarding the sharing of our personal information with smart devices that are able to monitor and store sensitive data. This being said, one must understand that the use of technological devices entails the collection of personal data from the user, most of the time. Such data can be sensitive as defined in clause 4.3.4 of the *PIPEDA*[2]. Hence, if such personal data is accessed without proper consent, it may breach user privacy rights. Moreover, if the information collected is of sensitive nature, it may increase the risk that harm is inflicted on the user such as discrimination or identity theft. However, not all smart devices pose a privacy threat because, as we shall see, some collect benign data; yet, the data generated from multiple interconnected devices can reveal sensitive information. As an example, a person can own a smart fridge, a wearable such as a smartwatch and a virtual assistant that uses AI algorithms such as Alexa. The quantity and the sensitivity of the information retrieved by these three items will greatly vary individually, but if their data is aggregated, they could reveal confidential information. Their popularity is also increasing. In fact, connected devices have already surpassed the number of people in the world and they are estimated to increase to 41.6 billion by 2025[3]. This is especially worrisome when considering how interconnected we are becoming through smart devices. Nonetheless, some of these devices such as wearables have numerous advantages. Indeed, wearables are no longer just used for sheer entertainment and are welcomed in "healthcare […] and security"[4]. They are

---

[1] David BURKE, "Why it is important to outsmart the smart devices", *CBC NEWS*, December 28, 2018, online: <https://www.cbc.ca/news/canada/nova-scotia/privacy-smart-speakers-google-amazon-smart-devices-1.4951026> (accessed on October 21, 2019).

[2] "[…] Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive", *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[3] Steve RANGER, "What is the IoT? Everything you need to know about the Internet of Things right now", *ZDNET*, February 3, 2020, online: <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/> (consulted on February 24, 2020).

[4] Vivian Genaro MOTTI and Kelly CAINE, "Users' Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected", in *Financial Cryptography and Data Security*, Berlin, Springer, 2015, online: <https://link.springer.com/chapter/10.1007/978-3-662-48051-9_17>, <https://www.researchgate.net/profile/Vivian_Motti/publication/271842005_Users'_Privacy_Concerns_About_Wea

easily accessible to the general public and they can be used in a variety of cases due, among other things, to their small size and functionality; but what are smart health devices such as wearables?

Smart health devices are first and foremost smart devices[5]. As we shall see in the first section of our thesis, there are multiple types of smart devices. These technological gadgets have a so-called *intelligence* defined by the scope of data they can sense, process and communicate[6]. Lee-Ann CONROD mentions three categories of smart devices[7] which will be presented in more detail in the first section of this thesis. To give a general overview, we shall enumerate the categories of smart devices available to the general population.

Essentially, the first category is composed of dumber or less intelligent devices that interact with their owners but do not reveal personal information other than what is computed by the device. Such devices can be considered a luxury such as a smart refrigerator, a smart plug, a smart kettle or any "smart" device that could be used without its "smart" feature. We will cover some of them throughout this thesis to demonstrate that such devices could cause more harm to their users than the perceived benefits. The users' collected personal data, even benign, becomes vulnerable to hackers and can be used by law enforcement to track a user's home activity, amongst other risks. Moreover, any risk arising from this category of devices is enhanced in the two following it, which is why the importance of covering this category should not be overlooked.

The second category of smart devices could potentially reveal sensitive information on its users[8]. While the previous category can reveal some personal information, the information retrieved by these devices is broad and ranges from finances to health and other data that could harm an individual if accessed without consent. This category is the one that most affects a user's privacy rights for the many reason which will be developed further on. As well, this category is the one

---

rables_impact_of_form_factor_sensors_and_type_of_data_collected/links/54d3eb290cf25013d027bbc0/Users-Privacy-Concerns-About-Wearables-impact-of-form-factor-sensors-and-type-of-data-collected.pdf>, point 2.1, (accessed on July 6, 2020).

[5] Smart devices are composed of all interconnected smart technology which includes smart health devices.

[6] Vivian Genaro MOTTI and Kelly CAINE, "Users' Privacy Concerns About Wearables", prev. cited, note 4.

[7] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", (2019) 24 *Appeal: Review of Current Law and Law Reform* 115, pp. 126ss, online: <http://www.canlii.org/t/sfd8> (accessed on October 28, 2019).

[8] *Id*., p. 130.

which is of the greatest interest to us because most smart health devices fall into this category such as those that will be the focus of this thesis. Smart health devices are mostly known to be wearable devices. Some examples include but are not limited to wearable fitness trackers, smart health watches, wearable ECG monitors, wearable blood pressure monitors, and biosensors[9]. These will be expanded on in part I of the thesis. These devices can also be perceived to be necessities by users and the medical community as they can work in conjunction with medical professionals to speed up health monitoring, increase the accuracy of diagnosis and help prevent diseases in users, as will be demonstrated in a later chapter. Nonetheless, these devices capture numerous details about a user's life and their lifestyle, being able to reveal their private medical information which poses privacy risks needed to be addressed.

The third and final category mentioned by the author is that of very smart devices[10]. These devices are advanced and can interact with their users while providing feedback. Some examples include but are not limited to: smart televisions equipped with cameras, computers and laptops or personal assistants such as Amazon's Alexa or the Google Home. The devices this category includes are capable of monitoring, storing and analyzing sensitive information on a user's lifestyle, even a user's health information; therefore, any risks with this category will also be addressed as they can be transposed to smart health devices. The biggest difference between the two is the amount of information collected and on whom.

Finally, it would be important to keep in mind that with the evolution of technology, any device can transcend into any of the three categories mentioned above. This concerns smart health devices, which will be our focus in this thesis, as they can transcend into any of the three categories and differently affect user privacy. We decided to focus on smart health devices because we believe that they are the ones that can benefit consumers the most in terms of functionality and health while also serving our public health system track down uprising health

[9] Alicia PHANEUF, "Latest trends in medical monitoring devices and wearable health technology", *BUSINESS INSIDER*, July 19, 2019, online: <https://www.businessinsider.com/wearable-technology-healthcare-medical-devices> (accessed on December 10, 2019); "A smart connected device/wearable for health is an electronic device or clothing article that automatically captures data on certain aspects of one's health or well-being, […] and then transfers these data to a mobile app on a smartphone or tablet, or to an application on a computer, for analysis", Guy PARÉ and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, Montreal, CEFFRIO, 2017, online: <https://www.benefitscanada.com/wp-content/uploads/2017/09/CanadaHealthInfoway_DiffusionofSmartDevicesforHealthinCanada.pdf> (accessed on May 26, 2020), p. 36.

[10] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: […]", prev. cited, note 7, p. 130.

concerns. As smart medical devises are, first and foremost, smart devices, general preoccupations regarding the data that is shared by these tools will remain pertinent.

With the right to privacy being our top concern in this thesis, we have established that different categories of smart devices entail a different expectation of privacy. Some can also be more invasive than others and reveal sensitive information on its users. Yet, we see the importance of smart health devices in healthcare as well as in public health and their potential to benefit both individual users and the collectivity. With climate change on the rise, so are infectious diseases[11]. The World Health Organization has noted an increase in infectious diseases which "reflects the combined impacts of rapid demographic, environmental, social, technological and other changes in our ways-of-living"[12]. The need for new monitoring and preventative mechanisms arises when considering the lives taken away by the flu, around 500,000 lives per year[13], and new viral outbreaks such as the ongoing COVID-19 pandemic; such viruses "aren't as unexpected as they might seem"[14] and their spread could be prevented if spotted early on. In fact, "their severity cannot be assessed in a timely manner, and thus, systems capable of providing estimates of influenza incidence are critical to allow health officials to properly prepare for and respond to influenza-like illness (ILI) outbreaks"[15].

While smart health device users can benefit individually from their gadgets, they are susceptible to a breach in their right to privacy which can, in some cases, violate their right to dignity, as will be seen. On the contrary, if our health data is put into good use, it can benefit us collectively. Some may believe that gathering and storing our personal information without consent is wrong, but what if this information can help save lives? We therefore want to balance the risks and benefits of using smart devices in healthcare for both the users and the Government and to see how doing so would affect our privacy rights.

---

[11] WORLD HEALTH ORGANIZATION, "Climate change and human health - risks and responses. Summary", online: <https://www.who.int/globalchange/summary/en/index5.html> (accessed on May 8, 2020).
[12] *Id*.
[13] Mauricio SANTILLANA, André T. NGUYEN, Mark DREDZE, Michael J. PAUL, Elaine O. NSOESIE, John S. BROWNSTEIN, "Combining Search, Social Media, and Traditional Data Sources to Improve Influenza Surveillance", (2015) *PLoS Comput Biol*.
[14] *Id*.
[15] *Id*.

We will demonstrate that such devices have the ability to improve public health but this does not come without its own set of risks. In fact, we shall see that the risks associated with smart health devices are mostly individual while the benefits are both individual and collective. Therefore, as will be discussed, the solution we propose to maximize the collective benefits and to ensure that data collection remains in the interest of a population is to create a national and international database generated by smart health devices capable of monitoring individuals' health and collecting data anonymously. The national database would be monitored by the Public Health Agency of Canada while the international database would be monitored by the World Health Organization. It would assist the Government and the WHO in making decisions quicker and more efficiently regarding arising health issues. Yet, the databases are mere solutions to a grander idea, which is to track diseases and flu-like-symptoms through wearables and smart health devices by using multimodal assessments through different devices and sources. The benefits of combining multiple data sources ranging from Google search queries, social media, hospital records, and traditional data sources to participatory surveillance have shown to improve Influenza and disease surveillance[16]. However, as we shall demonstrate, adding objective information retrieved by smart health devices is efficient in spotting upcoming viruses and tracking their spread. All this data combined outperforms each independent data source, predicts earlier with greater accuracy and the rate of accuracy is comparable to real-time predictions. We therefore push the idea further by adding wearables and smart devices into the calculation to further increase the accuracy and predictability of disease surveillance.

Indeed, "[e]arly warnings of disease outbreaks can help people and governments save lives"[17]. Even as early as December 2019, an AI in Boston was able to send out a first global alert informing of a new viral outbreak in China, the new Coronavirus. While humans were able to do the same but a bit later than the AI and while such devices can create many false positives, their usefulness in the medical field is undeniable. As of now, this AI that reported the outbreak of the Coronavirus was able to do so by scanning news and social media reports and ranked the alert a

[16] Mauricio SANTILLANA, André T. NGUYEN, Mark DREDZE, Michael J. PAUL, Elaine O. NSOESIE, John S. BROWNSTEIN, prev. cited, note 13.
[17] Matt O"BRIEN and Christina LARSON, "Can AI flag disease outbreaks faster than humans? Not quite", *AP NEWS*, February 19, 2020, online: <https://apnews.com/100fbb228c958f98d4c755b133112582> (consulted on March 17, 2020).

3 out of 5 based on the data analyzed[18]. While the ability of an AI analyzing existing data is promising, we believe that the problem stems from insufficient data on a country's overall health, especially considering that the media usually covers events once they happen and not in a preventative way. Hence, the AI that sent the alert for this new virus could not have known that a health epidemic was occurring before the media had time to cover it. As a matter of fact, as said by Nita MADHAV, CEO of San Francisco-based disease monitoring firm Metabiota, "the algorithms can only be as effective as the data they are scouring"[19]. Truly, we will see that smart health devices can indeed predict health problems before a licensed health practitioner can notice any signs. Therefore, we believe that creating a national and international database generated by these devices, used in conjunction with other methods available such as AI alerts, Google search queries[20] and much more, would allow to get a better representation of what is happening nationally and internationally in terms of health.

Although this is a complex issue due to the international custom of State sovereignty, we do nonetheless wish to present such an idea. Indeed, the sole fact that we were not quick enough to contain the COVID-19 outbreak before it became a pandemic suggests we need to consider new methods of disease surveillance. However, aside from the numerous additional benefits we believe such databases would provide, which shall be discussed later on in this thesis, we cannot help but discuss if the legal risks are worth it. Consequently, we will look at the risks and advantages both users of this technology and the Government might encounter in increasing the use of smart health devices and the data retrieved to improve overall health.

Throughout this thesis, we shall look at both the pros and cons of the increased use of smart health devices in order to determine whether the benefits of using them to improve overall health outweigh the consequences resulting in the infringement of our right to privacy by the Government or third parties whose interests do not always align with the concerns of citizens. Concerns with the right to privacy and to dignity come to the forefront when considering the impact their breach might have, especially if the information revealed is of sensitive nature. Such

---

[18] Matt O"BRIEN and Christina LARSON, "Can AI flag disease outbreaks faster than humans? Not quite", prev. cited, note 17.
[19] *Id*.
[20] Shihao YANG, Mauricio SANTILLANA, and S. C. KOU, "Accurate estimation of influenza epidemics using Google search data via ARGO", (2015) 112 *Proc Natl Acad Sci USA*, online: <https://www.pnas.org/content/112/47/14473> (consulted on May 7, 2020).

concerns might deter people from sharing their personal health information (PHI)[21] which can be crucial in public health. We will therefore tackle the dilemma of privacy versus health through the development of smart technologies to determine if generally speaking smart technologies pose a privacy threat to their users, thus putting at risk the users of smart health devices, or if such risks can be acceptable in exchange of better health assessments and an overall increase in collective health and wellbeing.

Nonetheless, we believe that a common interest resulting from an improvement in global health and perhaps quicker and better interventions from international organizations such as the WHO would outweigh the consequences of the infringement to our right to privacy; a right we already unknowingly give away through the Internet of Things (IoT)[22]. Indeed, users might not be aware of the data accessible through the devices which can pose privacy risks[23]. Notwithstanding, we believe that if an individual can benefit from quicker health assessments while saving time and money from the use of smart health devices, a whole population can benefit from the data extracted out of these devices to prevent health epidemics and avert their possible spread through the country and throughout the world. Thus, this thesis will explore whether the trade-off between health and privacy is a valuable one, when the personal information we unconsciously give away might both benefit us and limit our rights.

As we shall see, sharing our personal information does indeed have its advantages and disadvantages. The more users of smart technologies allow access into their personal lives by means of collected data, the better the collective datasets will become. However, this also entails that there will be a higher risk of privacy rights violations, along with other rights such as the right to dignity. It then becomes a legitimate concern to wonder if such access ought to be restrained to favor individual rights or broadened in the name of the common good. Moreover,

---

[21] *PIPEDA* defines personal health information as "information concerning the physical or mental health of the individual; […]", *Personal Information Protection and Electronic Documents Act*, prev.cited, note 2, article 2.

[22] The Internet of Things (IoT) refers to the interconnection of objects that can be controlled, which are usually know as smart devices, capable of connecting to the Internet and to each other, creating a giant network of connected things. They can communicate with other similar devices and with human beings. Feng XIA, Laurence T. YANG, Lizhe WANG and Alexey VINEL, "Internet of Things", (2012) 25 *Int. J. Commun. Syst*. 1101.

[23] Rani MOLLA, "People say they care about privacy but they continue to buy devices that can spy on them", *VOX*, May 13, 2019, online: <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security> (accessed on March 13, 2020).

by opening up this Pandora's Box, it could create a precedent where users of smart technologies will no longer be in control of their information nor to whom it goes and what is done of it.

Nonetheless, this thesis will demonstrate that, regardless of the numerous infringements of our right to privacy, amongst others, it is in the interest of all smart health device users to consent to sharing their personal data with a national and international database at the WHO. We believe that since users of these devices are already giving away their personal data to private entities such as Apple and Google, the stride between sharing such information from the private sector to the public sector is not so big, as long as the collaboration between these two sectors is possible. Partnerships could also be made such as it was recently done between Google and the WHO in relation to the new Coronavirus and the accuracy of the information online[24]. Indeed, the WHO partnered up with Google in order to ensure that the information shown in Google searches about the Coronavirus is accurate and that it stays so. These two agents have coordinated together to prevent false or misleading information by having the WHO's information seen in the top results. The WHO is also willing to partner up with other platforms such as Twitter and Facebook, amongst others, to prevent misinformation. Therefore, collaboration between the private sector and other public agents is likely.

To test our theory, we shall firstly go over the legal framework surrounding personal information and the right to privacy in Canada to see what protections are available in terms of privacy rights and what their limits are. We will proceed by reviewing both the risks and advantages the Government and users of smart devices will face if personal health data generated by smart devices were to be used in healthcare and aggregated into a national and international database. We will also cover the potential of smart technology and the benefits of using wearable devices individually in order to benefit a collectivity, whether it is to enhance health or safety. It is to be noted that while we will cover some governmental advantages, we will nonetheless focus on users of smart health devices as their consent and participation are essential for our solution to work. Doing so will allow us to weigh the pros and cons of sharing personal health data and determine whether the risks associated with it are worth the advantages; advantages that are not

[24] Madison DIBBLE, "World Health Organization partners with Google to stop spread of coronavirus misinformation", *WASHINGTON EXAMINER*, February 3, 2020, online: <https://www.washingtonexaminer.com/news/world-health-organization-partners-with-google-to-stop-spread-of-coronavirus-misinformation> (consulted on March 13, 2020).

only seen on an individual level but are also beneficial to a population and even to the world. To top it off, we will demonstrate the feasibility of using smart health devices in healthcare by consulting previous studies and innovations made using smart health devices and wearables.

Secondly, to cope with potential risks the Government and the users might face, we will explore some of the ways the latter can mitigate these risks such as through legal means, by themselves or through the action of appropriate authorities. Amongst the solutions to mitigate risks, we will cover the importance of informed consent which is a key consideration in insuring that smart health device users are willingly giving up some of their privacy rights. We shall see that informed consent is as much of an individual responsibility as it is a governmental one through the enforcement of proper consent practices by private enterprises prior to obtaining and sharing the information of smart device users. As for the Government and healthcare institutions, we will explain how to mitigate hacking risks which is a key concern in the health field. We will proceed by giving a solution that would benefit consumers, the Government, the WHO and different third parties. Apart from providing a solution, we will go into detail to explain how it will work and how the databases ought to be created, supported and maintained. Additionally, in order to emphasize the benefits both databases and smart health devices will bring to healthcare, we will further develop on how the Government and smart device users can favor their advantages. As for the Government, we will focus on the importance of a national database to help identify problematic areas of a country to allocate resources efficiently where needed and to make policies ensuring appropriate healthcare needs are met, but most importantly to track upcoming diseases and viruses through the use of smart health devices. We will also emphasize the importance of such a database for the WHO as it would allow the international organization to take a more efficient, timely and appropriate course of action when spotting early-on a potential outbreak. As for the users of smart health devices, we will focus on individual benefits of smart devices before explaining how a database can enhance their safety, security, efficiency of healthcare services and overall wellbeing.

Prescriptive Legal Positivism

The theoretical approach that will be used in this thesis is that of realism through the prism of prescriptive legal positivism in an attempt to understand the law as it is, but also how it ought to be in an evolving society. This approach will be the most relevant to our study because as mentioned by Braillard in *Théories des relations internationales*, realism is an objective observation of reality[25]. Hence, in order to make any suggestions regarding the state of law, it is important to have a non-biased and objective view of it beforehand, at least, as much as possible. Moreover, as this study will encompass both law and international relations, the theory of realism will be of relevance in analyzing the interactions amongst states and between them and its citizens. In addition, this essay will be inspired by the views of the 20th century legal philosopher Herbert HART who was one of the most influential defenders of legal positivism[26]. This, amongst many things, is a theory that suggests that law can be put to good and bad use, such as was noted by Hans KELSEN in *General Theory of Law and State* [27]. Law would then be described as a social means, but not an end[28]. Precisely, we will see how law both protects the people to whom it is applicable while turning against them when the opportunity arises. As well, we will see how it could be used honestly and maliciously. Furthermore, this paper will be in accordance with HART's separation thesis as described in *Positivism and the Separation of Law and Morals*[29]. In fact, not all which is legally permitted is so morally and vice versa. An extended perspective will be added, namely the inclusive legal positivism theory which allows for the consideration of moral values in assessing and determining what the law is or ought to be. Indeed, this idea was suggested by Ronald DWORKIN in *Law's Empire* who connected in part law to morality because it takes moral or evaluative judgments to interpret the law[30].

---

[25] Philippe BRAILLARD, *Théories des relations internationales*, Paris, Presses universitaires de France, 1977, 459 p., p. 69.

[26] Jean D'ASPREMONT, "Herbert Hart in today's international legal scholarship", in *International Legal Positivism in a Post-Modern World*, Cambridge, Jörg Kammerhofer, 2014, Cambridge University Press 114.
Also see: R.F. DEVLIN, "Mapping Legal Theory", (1994) 32 *Alta L. Rev*. 602, p. 605.

[27] Hans KELSEN, *General Theory of Law and State*, 1st ed., New York, Routledge, 2005, p. 5, online: <https://doi.org/10.4324/9780203790960>.

[28] *Id*., p. 20.

[29] H. L. A. HART, "Positivism and the Separation of Law and Morals", (1958) 71 *Harvard Law Review* 593, online: <http://users.umiacs.umd.edu/~horty/courses/readings/hart-1958-positivism-separation.pdf>.

[30] Ronald DWORKIN, *Law`s Empire*, Cambridge, London, Harvard University Press, 1986, 484 p., online: <http://www.filosoficas.unam.mx/~cruzparc/empire.pdf>.

I. Favoring the Greater Good: A Look into the Future

Smart Health Devices and their Impact on Privacy

While there are multiple types of smart devices, such devices have varying levels of so-called *intelligence* defined by the scope of data that such devices can sense, process and communicate[31]. Lee-Ann CONROD mentions three categories of smart devices[32]. The categories she creates are of relevance to this study as she uses them to distinguish what would constitute a violation of section 8 of the *Canadian Charter*[33]. This violation would infringe on an individual's right to privacy which is why it is important to tackle the issues that can arise with section 8 of the *Canadian Charter*. To prevent this violation, she also explains how the searches ought to be conducted in order not to violate users' reasonable expectation of privacy. Lee-Ann CONROD further demonstrates how the degree of intrusion will affect the conditions required to obtain a search warrant and proposes standards for privacy protection based on emerging technologies. She bases them on the criteria of intrusiveness, specificity, accuracy and the detail which is collected by the search. The first three criteria were developed in *R.* v. *A.M.*[34] in relation to sniffer dogs; the last one was added by the author to deal with new and emerging technology, in particular, smart devices, which shall be discussed throughout this thesis.

- **The first category** she refers to are smart devices that are inherently dumb[35]. They function as a smart device by being able to connect to the Internet or other smart devices, yet they do not interact with their owners. Examples of such devices are smart

[31] Vivian Genaro MOTTI and Kelly CAINE, "Users' Privacy Concerns About Wearables", prev. cited, note 4.
[32] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7.
[33] *Charte canadienne des droits et libertés,* partie 1 de la Loi constitutionnelle de 1982, [annexe B de la *Loi de 1982 sur le Canada,* 1982, c. 11 (R.-U.)].
[34] *R.* v. *A.M.,* [2008] 1 SCR 569, 2008 SCC 19 (CanLII).
It is to note that we define privacy based on Daniel J. SOLOVE's definition which is regrouped in six categories: "the right to be let alone; limited access to the self; secrecy; control of personal information; personhood; and intimacy", Daniel J. SOLOVE, "Conceptualizing Privacy" (2002) 90 *Cal. L. R.* 1087 p. 1095; K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", (2013) 65 *Droit et cultures* 191, para. 44, online: <https://journals.openedition.org/droitcultures/3092#ftn115> (accessed on May 23, 2020).
[35] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7, p. 128.

refrigerators, smart light bulbs, or smart kettles. While the information collected is stored in a database or a particular server, these devices do not usually reveal other personal information about their users other than the ones they are intended to collect like the amount of time a fridge door was opened in a day[36]. Although such information may be useful for an investigation, obtaining it would be minimally intrusive because law enforcement officers would not need to enter a home to access such information nor would they require anything from the users. It would be specific in nature as it would reveal only the information that was sought, not being capable of providing any other information and, as the data would be stored on a particular server, it remains much more accurate than human observation. The fourth category is the detail involved in the search and the conclusion with such devices is that it would be mundane, meaning it would not reveal a great deal about the users of these devices. Such data would not be considered as confidential information nor would it be sensitive in nature like personal health data would be. Therefore, we believe that the search of such devices, based on a reasonable suspicion in an investigation, would not violate a person's right to privacy. Hence, we would then not need to worry too much about the dumber smart devices and how their access may violate our fundamental rights. Nonetheless, as we shall see, dumber smart devices can also pose privacy risks, especially if used along with other smart devices. Any risks from this category can be applied to the following categories.

- **The second category** proposed by the author is the one where smart devices could potentially reveal sensitive information on its users[37]. This is where our fundamental rights come into play. They include but are not limited to smart watches and Fitbit's. As will be seen, these devices capture numerous details about a user's life and their lifestyle, being able to reveal their private medical information. Because of the sensitive nature of the personal data collected, such devices would require a higher degree of privacy than the ones from the previous category. However, any search of such devices would still remain minimally intrusive, specific in nature and have good accuracy for the same

[36] Indirectly, these devices may reveal other information such as a user's electricity consumption which could be linked to an illegal drug operation which may be noticed due to an important amount of electricity use.
[37] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7, p. 130.

reasons mentioned above. The problem arises with the new criteria added by Lee-Ann CONROD which is the detail that can be discovered on the user. When accessing the information stored by such devices, the information revealed can tell much more about the user than a search warrant can account for. Although we are looking at the invasion of a person's privacy though the scope of criminal investigations, the violation of a person's fundamental rights can be done by third parties and even by national or foreign governments. This only reiterates the importance of protecting personal data, and even so on some devices more than others. Such information ought to only be obtained by consent or by law enforcement based on a reasonable grounds standard along with prior judicial authorization.

- **The third category** proposed by the author is that of very smart devices[38]. Such devices are capable of interacting with their users and provide live feedback, whether through voice commands or through programming. Examples of these devices are smart televisions equipped with cameras, computers and laptops or personal assistants such as Amazon's Alexa or the Google Home. While this category does not necessarily include smart health devices, the devices it includes are capable of monitoring, storing and analyzing sensitive information on a user's lifestyle, even a user's health information. In fact, devices like Google Home save all search queries of its users. Just as the Google search engine, every input is collected, stored and is able to reveal more details on the users of such devices than they probably know themselves. This is because devices like these can listen to our commands but also to our ramblings and they are capable of recording an enormous amount of information, whether relevant to a search query or not. An example of such recording can be seen when browsing websites on a computer.

  Some websites install cookies[39] on a user's hard drive which means that it is possible to know which web pages where consulted by the user, even if it was an erroneous click. A

[38] Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7, p. 130.

[39] Cookies are small text files saved on a user's hard drive by a Web server. They remember a user's preference and information accessed. For more information on cookies see: Amir M. HORMOZI, "Cookies and Privacy", (2005) 13 *Information Systems Security* 51; Christopher SCOTT, "Our Digital Selves: Privacy Issues in Online Behavioural Advertising", (2012) 17 *Appeal: Review of Current Law and Law Reform* 63, on page 64.

simple web consultation on dog food might result in future ads for dog related products[40]. The problem worsens when these websites using cookies collect personal health information and use it to display advertisements which may reveal this information, such as was the case in a complaint to the Privacy Commissioner of Canada in early 2013[41]. In this particular case, the complainant had searched online for medical devices and following his search queries, he was targeted by advertisements from Google's AdSense service that revealed sensitive information about his health. This means that a breach in one's privacy can occur even before a smart health device is purchased simply by searching for one online. More so, while cookies would seem to allow a person to remain anonymous[42], the truth is that anonymity does not hinder the possibility of tracking back online activities and personally identifiable information back to the users, making it possible to identify them based on the data that is openly available.

Moreover, such devices end up knowing so much about their users' lifestyle that any search of these devices might amount to an invasion of privacy. Truly, searching these devices would undoubtedly violate one's privacy as it is impossible to separate relevant from irrelevant information; everything on a person's life would be accessible and even information on other individuals who were not subject to the search. In addition, such devices can be paired with smart health devices, thus potentially being able to expose sensitive health information if seized[43]. Similarly to the previous category, there should be reasonable and probable grounds that an offence will or has been committed to search the devices. A warrant should also specify the exact information sought by law enforcement officers. As technology becomes smarter, laws should become stricter.

---

[40] This type of problem has previously been reported to the Office of the Privacy Commissioner of Canada. See: *Use of sensitive health information for targeting of Google ads raises privacy concerns*, 2014 CanLII 3357 (PCC), par. 16, online: <http://canlii.ca/t/g2wqw>.
[41] *Id*.
[42] Eloïse GRATTON, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, Toronto, CCH Canadian, 2003, p. 46.
[43] As an example, the Apple watch is usually connected to the Apple phone through an application on the device.

As for smart health devices in particular, these are mostly known to be wearable devices. Some examples include but are not limited to wearable fitness trackers, smart health watches, wearable ECG monitors, wearable blood pressure monitors, and biosensors[44].

Wearable Fitness Trackers

Wearable fitness trackers compute a user's physical activity and heart rate while also providing feedback by syncing to other smartphone apps. The most commonly known fitness tracker is the Fitbit. The Fitbit was originally created to track a user's number of footsteps in a day and therefore increase their activity level by pushing the users to walk a greater distance daily.

Smart Health Watches

Another commonly known smart health device is the smart watch. It once held the same functionality as the Fitbit: to count steps and tell time; it is now used as a healthcare device. Indeed, this device not only has the functionality of a smart phone, but it can also track health related issues. One of the many brands available is the Apple watch. In fact, in 2017, Apple launched the Apple Heart Study app capable of monitoring the heart rate of its users and of alerting them when they were experiencing atrial fibrillation. In early 2019, Stanford Medicine researchers, in collaboration with Apple, presented the findings of their Apple Heart Study[45]. This study encompassed over 400,000 participants from all 50 states of the United States. The app would occasionally check the users' heart's rhythm to try to catch an irregular heart rate which would suggest atrial fibrillation. When an irregular heart rate was identified by the device, the users would receive a notification on their Apple Watch and their mobile device along with a telehealth consultation with a medical provider and received an electrocardiogram (ECG) patch

[44] Alicia PHANEUF, "Latest trends in medical monitoring devices and wearable health technology", prev. cited, note 9. Guy PARÉ and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 36.
[45] APPLE NEWSROOM, "Stanford Medicine announces results of unprecedented Apple Heart Study", March 16, 2019, online: <https://www.apple.com/newsroom/2019/03/stanford-medicine-announces-results-of-unprecedented-apple-heart-study/> (consulted on December 10, 2019).

to further monitor them. This allowed the users of such device to receive important health information before it could have been noticed by a doctor[46].

Wearable ECG Monitors

Also, similar to smart watches are wearable ECG monitors. These devices can measure electrocardiograms and send the results straight to the user's doctor. They can detect atrial fibrillation. Moreover, they are able to track a user's pace, the distance walked, the elevation and they automatically record movements such as "walking, running, swimming, and biking"[47].

Wearable Blood Pressure Monitors

In the same line of products, wearable blood pressure monitors have made their appearance, such as the Omron Healthcare which launched HeartGuide in 2019, becoming the first ever wearable oscillometric blood pressure monitoring device. It not only measures blood pressure as its title would suggest, but it can also record a user's physical activity such as the number of steps taken in a day, the distance traveled and the amount of calories the user has burned. With the data generated, the users can choose to transfer it to the Heart*Advisor* app to review it, to store it or to share it with their physician. This app also allows the users to get an insight on their habits and how they can affect their blood pressure[48].

Biosensors

Another smart health device is the biosensor. It is radically different from the previous devices as it does not come in the form of a wristband nor a watch. It is rather a self-adhesive patch that allows for the collection of data on the user's movements, heart rate, temperature and respiratory rate. The Philips' wearable biosensor is a great example. When computing the user's information, the data analyzed can be transmitted to the user's medical health provider through

---

[46] APPLE NEWSROOM, "Stanford Medicine announces results of unprecedented Apple Heart Study", prev. cited, note 45.
[47] Alicia PHANEUF, "Latest trends in medical monitoring devices […]", prev. cited, note 9.
[48] OMRON, "Heart Guide", online: <https://omronhealthcare.com/products/heartguide-wearable-blood-pressure-monitor-bp8000m/?utm_source=cj&utm_medium=affiliate&cjevent=6166a59f1bc911ea829c01520a24060b> (accessed on December 10, 2019).

advanced algorithms and inform the latter of the patient's condition[49]. As a matter of fact, the research provided by the Augusta University Medical Center (AUMC) revealed that wearable devices using these biosensors can predict when a patient's health condition worsens and is deteriorating. The Augusta Medical Center is actually one of the first to use wearable technology to improve patients' health by monitoring particularly at risk patients. This smart device with biosensors provides continuous and real-time data which alleviates some of the work that nurses have to do. The way it works in the hospital is that the wearable biosensor adheres to the patient's chest and transmits the data generated to a Bluetooth device and eventually this data is transmitted into the electronic medical record of the patient. As a result, it was able to reduce by 89% patients' deterioration into cardiac or pulmonary arrest, both being preventable conditions[50]. In essence, this product improved patients' diagnosis while reducing the amount of work nurses and other staff needed to do. Yet, amongst the many benefits are risks of using these devices.

A. The Risks of Using Smart Health Devices Individually and Collectively

As once said by Massimo ORSINI in the *Montreal Gazette*: "Ultimately, your risk is determined by what information you are willing to share, and the cost you are willing to pay for convenience"[51]. The infringement of our right to privacy from the use of smart health devices is one of the biggest concerns that we shall tackle in this thesis. Yet, privacy would be a cost to pay in order to find the equilibrium with public wellbeing by compromising privacy for greater health. However, before jumping into our analysis, it would be important to qualify personal information and the laws that cover the protection of personal data. We shall however restrict our analysis to Canada but will keep in mind the effects of international legislation such as the GDPR on Canada[52]. We decided to focus on Canada as a whole instead of focusing on one

---

[49] PHILIPS, "Philips wearable biosensor: Keep watch, know more, respond quickly", online: <https://www.usa.philips.com/healthcare/clinical-solutions/early-warning-scoring/wireless-biosensor> (accessed on December 10, 2019).

[50] Heather LANDI, "At Augusta University Health, Wearable Technology Enables Real-Time Monitoring of At-Risk Patients", *HEA!THCARE INNOVATION*, April 7, 2017, online: <https://www.hcinnovationgroup.com/clinical-it/article/13028366/at-augusta-university-health-wearable-technology-enables-realtime-monitoring-of-atrisk-patients> (accessed on December 11, 2019).

[51] Massimo ORSINI, "Opinion: Internet of Things poses privacy risks", *MONTREAL GAZETTE*, December 21, 2017, online: <https://montrealgazette.com/opinion/opinion-internet-of-things-poses-privacy-risks> (consulted on October 18, 2019).

[52] In Europe, the General Data Protection Regulations (GDPR) set an example by obliging smart device manufacturers and anyone who collects data to meet certain privacy regulations such as: limiting the collection of

province because, while the laws surrounding the protection of personal information in Canada are not exactly uniform from province to province, all provincial laws have to be similar to *PIPEDA*; therefore, all Canadians remain subject to the same general obligations.

1. Risks for Canadian Citizens

a) Legal Coverage of Personal Information in Canada

To understand the scope of the risks in regards to the protection of personal information[53] it is important to understand its legal framework in Canada along with the definition of personal information. To understand what personal information is, one must first consult its definition. In

---

personal data to what is necessary and for a well-defined purpose, informing users of harmful data breaches, allowing individuals to access data regarding them, processing data in a secure and confidential way, getting consent before collecting data, and deleting individuals' information due to their "right to be forgotten", Steve BELL, "Your privacy rights, GDPR and smart devices", *BULLGUARD BLOG*, December 11, 2017, online: <https://www.bullguard.com/blog/2017/12/your-privacy-rights,-gdpr-and-smart-devices> (accessed on October 20, 2019).
Also see: Fiona BRIMBLECOMBE and Gavin PHILLIPSON, "Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression", (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 1.
Also see: EUROPEAN COMMISSION, "A new era for data protection in the EU: What changes after May 2018", online: <https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf> (accessed on October 20, 2019).
Such models of protection of personal data, whether in Canada, in Quebec, or in the European Union, abide by the principles of: informed consent, collection of only relevant information and proportionate to its purposes, confidentiality, security, right of access, of rectification and to information, Florimond ÉPÉE, "La protection des données personnelles au Canada à l'ère des données massives", *Laboratoire de CYBERJUSTICE*, July 24, 2018, online : <https://www.cyberjustice.ca/actualites/2018/07/24/la-protection-des-donnees-personnelles-au-canada-a-lere-des-donnees-massives/> (accessed on October 24, 2019).
The principles of the federal and provincial legislation, similar to those of the GDPR, were inspired by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, online: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm > (accessed on October 24, 2019).
Also see: Florimond ÉPÉE, "La protection des données personnelles au Canada à l'ère des données massives", *Ibid*.
It is interesting to note that the GDPR has extra-territorial effects in regards to EU citizens. Moreover, *PIPEDA* was in line with the privacy standards for personal information as they have been developed by the European Union based on the highest international standards; a revision might currently be required as the last decision confirming that Canada is "providing an adequate level of protection of personal data transferred from the European Union (EU) to recipients subject to the Personal Information Protection and Electronic Documents Act (PIPEDA)" dates back to 2006. GOVERNMENT OF CANADA, "Fifth Update Report on Developments in Data Protection Law in Canada", June 2019, online: <https://www.ic.gc.ca/eic/site/113.nsf/eng/h_07666.html> (consulted on March 30, 2020).

[53] Depending on the laws we consult, our personal information could be considered as confidential information, but there are cases where we oppose personal information to confidential information. *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1., article 20; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c A-2.1, article 53; *Loi sur la Santé publique*, RLRQ, c S-2.2., article 95. The qualification entails different legal obligations for both the giver of the information and the holder of such information. Since both entail a different legal framework, we shall consider them as separate.

Canada, it is *the Personal Information Protection and Electronic Documents Act (PIPEDA)*[54] that applies. It defines personal information as "information about an identifiable individual", and it also provides us with a definition of personal health information which is defined as "information concerning the physical or mental health of the individual; […]"[55]. There are other similar definitions of personal information[56]; however, to summarize, it is any information such as a name, an address or a geographic location related to a person that serves to identify a person who has or could be identified with or without other data pieces. This definition has also been confirmed by the Office of the Privacy Commissioner of Canada[57].

It is now important to understand how the legal framework surrounding the protection of personal information works in Canada. There are laws and regulations in Canada pertaining to the protection of personal information. In fact, on the federal level, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*[58] serves as a basis for the protection of personal data, including health data. It applies to all provinces if they have not already established a similar law[59], and allows provinces, under section 26 (2) (b) of *PIPEDA*, to establish their own law if it is deemed "substantially similar" to *PIPEDA*[60]. Indeed, every province except for Alberta, British Columbia and Quebec, have to apply this law. The province

---

[54] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 2.

[55] *Id*., article 2.

To note, this definition is not perfectly identical to the provincial legislation of Alberta, British Columbia and Quebec, but that this definition is relatively similar.

[56] OECD defines it as "any information relating to an identified or identifiable individual", OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, prev. cited, note 52.

As for a more detailed definition of personal information, the General Data Protection Regulation defines it as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", *EC, Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* [2016] OJ, L 119/1 [GDPR], article 4, online: <https://gdpr-info.eu/art-4-gdpr/> (accessed on October 19, 2019).

[57] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Summary of privacy laws in Canada", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/> (accessed on September 25 2019).

[58] *Personal Information Protection and Electronic Documents Act*, *Ibid*.

[59] Florimond ÉPÉE, "La protection des données personnelles au Canada à l'ère des données massives", prev. cited, note 52.

[60] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Provincial legislation deemed substantially similar to PIPEDA", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/> (accessed on September 25, 2019).

of Quebec has adopted the following law: the *Act respecting the protection of personal information in the private sector*[61], which is deemed substantially similar to *PIPEDA*[62]. As for the other two provinces that have substantially similar laws, namely Albert and British Columbia, the first has adopted the *Personal Information Protection Act* (PIPA)[63], while the latter has adopted the *Personal Information Protection Act*[64]. Furthermore, in regards to health, some provinces have adopted health-related privacy laws similar to *PIPEDA* and are therefore partially exempt from it[65]. *PIPEDA* will therefore not apply to private health providers that operate within these jurisdictions, but will apply to commercial activity therein. Other provinces do have their own privacy health laws but they are not substantially similar to the *PIPEDA*[66]. Furthermore, as for the obligation to protect personal health data particularly, Quebec has adopted the *Act respecting health services and social services*[67], the *Health Insurance Act*[68], and the *Act respecting the Régie de l'assurance maladie du Québec*[69].

PIPEDA abides by ten principles which are both mandatory obligations and recommended practices:

> "**Accountability**: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

---

[61] *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1.
[62] Moreover, although not related to *PIPEDA* but still interesting to take note of, Quebec has also adopted the *Act respecting Access to documents held by public bodies and the Protection of personal information* which will nonetheless continue to apply to federally-regulated businesses in the province in regards to the protection of personal information, *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1.
[63] *Personal Information Protection Act*, S.A. 2003, c. P-6.5.
[64] *Personal Information Protection Act*, S.B.C. 2003, c. 63.
[65] Ontario has adopted the *Personal Health Information Protection Act*, *Personal Health Information Protection Act*, 2004, SO 2004, c. 3, Sch A.;
New Brunswick has adopted the *Personal Health Information Privacy and Access Act*, *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05.;
Newfoundland and Labrador has adopted the *Personal Health Information Act*, *Personal Health Information Act*, SNL 2008, c. P-7.01;
Nova Scotia having adopted the *Personal Health Information Act (PHIA)*, *Personal Health Information Act,* SNS 2010, c 41.
[66] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Summary of privacy laws in Canada", prev. cited, note 57.
[67] *Act respecting health services and social services*, CQLR, c. S-4.2. See sections 19 (13) and 520.1 for health information.
[68] *Health Insurance Act*, CQLR, c. A-29. See section 65.0.3. for health information.
[69] *Act respecting the Régie de l'assurance maladie du Québec*, CQLR, c. R-5. See section 2 (k) for health information.

Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

> **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance"[70].

Notwithstanding, it is to note that *PIPEDA* also applies to federally-regulated businesses such as airlines, banks, railways, telecommunication companies and service providers but does not apply to non-profit organizations, charities or political parties. Yet, *PIPEDA* is not the only law regulating the protection of personal information in Canada. Indeed, while *PIPEDA* covers how businesses ought to handle personal information, the *Privacy Act*[71] applies to the federal government. The latter allows an individual not only to access their personal information held by the Government, but also to correct it while setting guidelines as to the collection, the use and the disclosure of such information. Nevertheless, our privacy laws, namely *PIPEDA*, have been criticized on their ability to respond to modern technological challenges[72]; although, as we shall demonstrate, some recent changes may point otherwise.

b) Risks of Personal Information Being Accessed

For starters, large quantities of data are already processed through different kinds of sources[73] every day on top of the data collected by wearable devices. This information is for the most part collected about people regarding their "characteristics, their thoughts, their movements, behaviour, communications, and preferences – or they can be used to produce such data"[74]. This information is gathered by different kinds of information processors which can be either human or artificial[75]. The ones we are concerned about are the artificial types of processors, namely smart technologies.

---

[70] Tariq AHMAD, "Online Privacy Law: Canada", *LIBRARY OF CONGRESS*, June 2012, online: <https://www.loc.gov/law/help/online-privacy-law/2012/canada.php> (consulted on March 26, 2020).
[71] *Privacy Act*, R.S.C. 1985, c. P-21.
[72] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Summary of privacy laws in Canada", prev. cited, note 57. Also see : K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 41.
[73] "[s]earch engines, satellites, sensor networks, scientists, security agencies, marketers, and database managers", Jeroen VAN DEN HOVEN, "Information Technology, Privacy, and the Protection of Personal Data", (2008) *Information Technology and Moral Philosophy* 301, p. 301.
[74] *Id*.
[75] *Id*., p. 307.

As technology evolves, it makes our lives much more convenient as we buy into it, connecting to the Internet of Things (loT); however, "possibilities widely exist for the personal data to be collected inappropriately" and "IoT-based applications are extremely vulnerable due to two basic factors: (1) most of the communications are wireless, which makes eavesdropping extremely simple; (2) most of the IoT components are characterized by low energy and low computing capabilities, thus they can hardly implement complex schemes on their own to ensure security"[76]. Nevertheless, we connect to the IoT disregarding our personal information and how it is collected and used. Without knowing it, our smart devices are able to profile us based on the inputs we provide them, such as our eating habits monitored by a smart refrigerator, or our viewing habits monitored by our smart television, to name a few. While the latter are minimally intrusive and do not reveal sensitive information, other devices can also monitor us without us having to give them any inputs. Let's take shopping for example. We might think cameras are our biggest problem in monitoring our activities; however, laws prohibit the collection of data on people longer than necessary[77]. Yet, our devices, namely our smart health devices, can collect and store our personal information continuously. While a camera recording will eventually be discarded, our health data, gathered from such devices, is continuously registered and updated. The worry for privacy then does not derive from a camera in a store but from the devices we carry on ourselves such as our mobile device. To illustrate this point, retailers are now able to tap into them if the Wi-Fi or Bluetooth feature is left on and thus monitor our activities as we walk through the mall[78]. The harvested data can inform them of our shopping patterns such as the time we spend in a particular store, in what isles we shop and what products we buy.

---

[76] For the initial definition of IoT, please refer to note 22.
"IoT consists of a set of technologies to support the communication and interaction among a broad range of networked devices and appliances", Yuehong YIN, Yan ZENG, Xing CHEN, and Yuanjie FAN, "The internet of things in healthcare: An overview", (2016) 1 *J Ind Inf Integr* 3, online: <https://www.sciencedirect.com/science/article/pii/S2452414X16000066> (accessed on May 23, 2020);
Steve TAN, "How safe is your personal data collected by your smart devices?", *BUSINESS TIMES*, September 18, 2018, online: <https://www.businesstimes.com.sg/opinion/how-safe-is-your-personal-data-collected-by-your-smart-devices> (accessed on March 20, 2019).

[77] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Guidelines for Overt Video Surveillance in the Private Sector", March 2008, online: <https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gl_vs_080306/> (accessed on March 20, 2019).

[78] Steve TAN, "How safe is your personal data collected by your smart devices?", *Ibid*.

If it sounds familiar, that is because there is a possible case involving Target and other malls in Canada[79]. Target shall be used as an example to demonstrate the severity of the concern even if the allegations are disputed. Although the story may be fictitious, it illustrates real life concerns from the use of portable devices. In fact, Target had assigned every customer a Guest ID which in turn was tied to their personal information such as their credit card, their name or email address, which were all collected and stored, without being deleted. Yet, the main issue with the case regarding Target was the breach of personal information done by the company itself, mainly by Target's statistician Andrew Pole. He allegedly created a pattern meant to figure out at what trimester women were and catered coupons to them accordingly[80]. One particular case was the one of a father of a high school girl that received coupons for baby clothes and cribs. He was outraged that someone would send her such coupons promoting pregnancy in young women; however, he realized afterwards, that way, that his daughter was indeed pregnant[81]. Essentially, this example illustrates how the collection of data can negatively impact someone. Moreover, this goes on to show that the data regarding consumers' health and consumption can be used against them, if not consensually provided. In theory, such data could have been seized through smart health devices connected with Bluetooth or Wi-Fi to a cellular device.

Yet, one of the biggest issues with such collection of data can be summarized with the case of TJX[82]. In 2007, TJX was the victim of a network computer intrusion that affected the personal information of around 45 million payments cards in five countries including Canada. This

---

[79] Kashmir HILL, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", *FORBES*, February 16, 2012, online: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#210ffc4a6668> (accessed on March 20, 2019); Sarah RIEGER, "At least two malls are using facial recognition technology to track shoppers' ages and genders without telling", *CBC NEWS*, July 26, 2018, online: <https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964> (accessed on August 27, 2020); Anis HEYDARI, "Cellphone tracking has been used in at least 1 Canadian mall, former employee says", *CBC NEWS*, August 7, 2018, online: <https://www.cbc.ca/news/canada/calgary/cadillac-fairview-mall-location-tracking-1.4775990> (accessed on August 27, 2020).
Also see: Rachel ABRAMS, "Target to Pay $18.5 Million to 47 States in Security Breach Settlement", *THE NEW YORK TIMES*, May 23, 2017, online: <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html> (accessed on April 4, 2019).

[80] It is to note that the claim that Target had figured out a way to know if someone is pregnant before there were any signs is disputed. Colin FRASER, "Target didn't figure out a teenager was pregnant before her father did, and that one article that said they did was silly and bad", *MEDIUM*, January 3, 2020, online: <https://medium.com/@colin.fraser/target-didnt-figure-out-a-teen-girl-was-pregnant-before-her-father-did-a6be13b973a5> (accessed on March 17, 2020).

[81] Kashmir HILL, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", *Ibid*..

[82] *Report of an Investigation into the Security, Collection and Retention of Personal Information*, 2007 CanLII 41283 (PPC).

experience demonstrates how maintaining a large amount of "sensitive information"[83] could become a liability, especially if the information kept no longer serves the purpose it intended to and is kept longer than necessary. Moreover, "collecting and retaining excessive personal information creates an unnecessary security burden"[84]. The lesson learned was that a company ought to not retain unnecessary personal information nor collect it; a lesson that TJX learned the hard way. This is confirmed in Principle 5 of *PIPEDA*. It is similar to section 6 of the *Privacy Act*, but for government institutions. A comparison we would like to make is with the idea of having a national and international database[85]. While allegedly more secure than TJX's computer network, these databases would need to keep personal sensitive information for long periods of time to analyze the progression of a disease. Thus, keeping personal health information stored in such a database could be a risk for both the Government and the citizens. The upside is that data would be generated anonymously, but while it is anonymous, it is still retraceable. Currently, there are also no laws specifically protecting anonymous information[86] and it would not fall under the obligation of being discarded after a reasonable time.

In addition, amongst many methods available such as hacking, one of the biggest vulnerabilities of smart devices is the possibility to access them through their Wi-Fi password[87]. On smart kettles, for example, or any similar item, people do not change their default username or password. Being available on the internet, people may use these passwords to access a device and connect to the Wi-Fi network. Once in it, it is possible to monitor the activity that is done online, including getting access to confidential information such as finances. As we shall see, this information to hackers is of value and there is a lucrative market for health information. Yet, the main attraction is the possibility to access payment information, names, messages and phone numbers in smartwatches in comparison to fitness trackers who store a limited amount of information[88]. If access to personal data cannot be as easily achieved, then hacking is definitely an option for the determined minds. If hackers are able to remotely unlock a smart door using

---

[83] *Report of an Investigation into the Security, Collection and Retention of Personal Information*, prev. cited, note 82, par. 3.
[84] *Id*.
[85] This idea will be explained in part II of our thesis.
[86] See *Loi concernant le cadre juridique des technologies de l'information*, prev. cited, note 52, section 25.
[87] David BURKE, "Why it is important to outsmart the smart devices", prev. cited, note 1.
[88] Lisa EADICICCO, "This Giant Security Hole Could Affect A Huge Chunk Of The 'Secure' Web", *BUSINESS INSIDER*, April 8, 2014, online: <https://www.businessinsider.com/heartbleed-security-flaw-2014-4> (accessed on October 21, 2019).

limited equipment and a phishing email, and access people's Wi-Fi by doing so, connecting to all their connected smart devices[89], they could just as well hack into wearables or any other smart health device. The information collected would be sensitive and could reveal a lot about the users of such devices, from their lifestyle to their health problems. As seen earlier, smart health devices have the same options as *dumber* devices but surpass them in terms of data collected and the sensitive nature of it. If there are risks for smart kettles, which are known as the *dumber* smart devices, such risks can easily be transposed to smart health devices and wearables.

Our personal information is also of value to third parties in order to make a profit out of it, one way or another. Advanced smart devices using artificial intelligence such as Google Home and Amazon Echo can learn a great deal about their users, from their habits to their conversations[90]. Catherine TULLY, Nova Scotia's former information and privacy commissioner, mentioned that these devices are mainly created to access important personal information to be sold for marketing purposes. As for Google, it denies that its AI technology stores any information but the one received after a command has been prompted such as "Ok Google". It also denies selling people's personal data to third parties. However, as we shall see, these smart devices do listen to us or minimally capture key words to initiate the recording process. This concern will reappear when discussing wearables such as a Fitbit or the Apple watch. As we shall see, while smart health devices do not necessarily interact with their user like advanced smart devices do, they nonetheless can compute as much data without the user's knowledge[91].

On a brighter note, wearables could also boost employee productivity by up to 8.5% and raise their job satisfaction by 3.5%[92]. The problem, however, is that wearables, mainly used for health purposes, require an app; apps are more likely to have data breaches because all the data they collect is stored in one place. This is without mentioning the greater problem: apps record our location, where we have been and how many times we have visited a place such as a doctor's

---

[89] Luke DENNE, Greg SADLER and Makda GHEBRESLASSIE, "We hired ethical hackers to hack a family's smart home — here's how it turned out", *CBC NEWS*, September 28, 2018, online: <https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963> (accessed on March 27, 2019).

[90] David BURKE, "Why it is important to outsmart the smart devices", prev. cited, note 1.

[91] *Id*.

[92] Rhiannon WILLIAMS, "Wearables can boost employee productivity by almost 10pc", *THE TELEGRAPH*, May 1, 2014, online: <https://www.telegraph.co.uk/technology/news/10801687/Wearables-can-boost-employee-productivity-by-almost-10pc.html> (accessed on March 21, 2019).
To be noted that employers cannot impose such devices as they permit tracking, as seen in article 47 of the *LCCJTI*.

office[93]. This information could be shared with third parties such as companies due to the "authorization" by the user who enabled location services to benefit from a particular app such as a weather app[94]. The companies that access this data use it to cater it to other third parties such as advertisers who want an insight into consumer behavior. Also, since consent is needed to access personal information and to distribute it, apps may request such an access in exchange of services provided by the app, many times buried in vague privacy policies. Some companies even use health information to run ad campaigns for personal injury lawyers who target people in emergency rooms[95]. If such information were to be accessible to them through wearable devices, they could use it for the same purpose which could breach a user's right to privacy. The fact that health data is sought out by different parties shows how vulnerable users can be of a privacy breach when using smart health devices. The *New York Times* estimates that Google's Android has over 1,200 apps with a location-sharing code, whereas Apple's iOS has roughly 200. Our smart devices give third parties access to our personal data through apps and a collection of software installed on them; if such devices have an Internet service provider, than the latter might be violating Canadian privacy laws[96]. They are not as transparent as we think.

Once our information is accessed and data is stored, it is quite normal to desire an accurate representation of our information, especially when shared publically. Yet, another problem with smart devices is that they constantly stock personal data. A user has a right to control their personal information and for it to accurately represent him or her[97]. As smart health technologies constantly gather data and metadata, they may provide inaccurate information about the user that cannot be rectified. In fact, the use of such devices would generate a ton of automatically

---

[93] Jennifer VALENTINO-DEVRIES, Natasha SINGER, Michael H. KELLER and Aaron KROLIK, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *NY TIMES*, December 10, 2018, online: <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html > (accessed on March 21, 2019).

[94] This was the case with AccuWeather's IOS app, Taylor HATMAKER, "Users dump AccuWeather iPhone app after learning it sends location data to a third party", *TECHCRUNCH*, 2017, online: <https://techcrunch.com/2017/08/22/accuweather-revealmobile-ios/?ncid=rss> (accessed on March 21, 2019).

[95] Jennifer VALENTINO-DEVRIES, et. al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *Ibid*.

[96] Andrew CLEMENT and Jonathan A. OBAR, "Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers", (2016) 6 *Journal of Information Policy* 294.

[97] Pierre TRUDEL, *Le droit de l'information : une introduction*, Montréal, 2017, 17 p., on page 5, online : <https://pierretrudel.openum.ca/files/sites/6/2017/07/DroitdelinformationINTRO.pdf> (accessed on March 24, 2019).
Also see: *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.
Also see : *Loi concernant le cadre juridique des technologies de l'information*, prev. cited, note 52, article 23.

generated data that cannot be tampered with[98]. The users are also unable to destroy personal information that is recorded of them[99], while such right is guaranteed in the EU under the GDPR. In Canada, there is a similar right to destroy documents under section 6 (2) of the *Act to establish a legal framework for information technology*[100]. However, there is no right to be forgotten in Canada such as it has been developed in the EU; nonetheless Bill 64 might introduce this right to Canadians[101]. Although *PIPEDA* mimics the rules set out by the GDPR, this right is only guaranteed in the European Union, for now[102]. This means that users cannot yet have access or control the information kept about them, meaning that such information could be leaked and even used against the latter. However, Bill 64 greatly increases the rights these users have by also including the right to be forgotten such as it is codified in section 17 of the GDPR.

The problem mentioned previously brings up another one which is that there is a risk of an invasion of privacy when information can be deduced by the metadata gathered by smart health devices. While computers might reveal our most private desires, smart devices that track our bodily movements would be able to register in their metadata what activities are being performed inside of a house, such as in a bedroom behind closed doors[103]. While analyzing data from smart health devices that is of relevance in a Court setting, there is no avoiding such an encounter in order to sort out the relevant information. The data that could be revealed is considered highly

---

[98] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies in Healthcare and the Law", (2018) 27 *Dalhousie Journal of Legal Studies* 59, p. 83.
[99] *Id*., p. 83.
[100] *Loi concernant le cadre juridique des technologies de l'information*, prev. cited, note 52, article 6, para. 2.
[101] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Projet de loi n° 64, 1ière session, 42e légis. (Can.)., online : <http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html> (accessed on July 23, 2020); Simon DU PERRON, "Projet de loi 64 : une réforme à l'Européenne du droit à la protection des renseignements personnels", *CYBERJUSTICE LABORATORY*, June 17, 2020, online : <https://www.cyberjustice.ca/2020/06/17/projet-de-loi-64-une-reforme-a-leuropeenne-du-droit-a-la-protection-des-renseignements-personnels/> (accessed on July 23, 2020).
[102] Martin UNTERSINGER, "Le « droit à l'oubli » ne s'applique pas au monde entier, tranche la justice européenne", *LE MONDE*, September 24, 2019, online: <https://www.lemonde.fr/pixels/article/2019/09/24/le-droit-a-l-oubli-ne-s-applique-pas-au-monde-entier-tranche-la-justice-europeenne_6012818_4408996.html> (accessed on October 18, 2019). Indeed, this has been decided in September 2019 by the Court of Justice of the European Union that restricted this right to the Member States of the EU. *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, Affaire C-507/17, September 24, 2019, online: <http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0507&lang1=fr&type=TXT&ancre=>. Moreover, this right is not guaranteed all over the world, even for the citizens of the EU. The right to dereference, as it is called, only applies to domain names of the European Union such as "Google.fr", linked to the proper IP address, but the removed information could still be accessible through other domain names like "Google.com"; K. BENYEKHLEF, et. al., "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 74-77.
[103] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", *Ibid*., p. 96.
See note 156: the OPC is favoring adding the right to be forgotten into Canadian legislation as it exists in the EU.

private, whether from our browser searches to our bodily sensory outputs, especially if it is combined with location information[104], and can infringe on one's right to dignity.

Additionally, speaking of dignity, it is also one of our fundamental rights. Dignity is guaranteed under section 4 of the *Quebec Charter of Rights and Freedom*[105] which reads "4. Every person has a right to the safeguard of his dignity, honour and reputation"; it is not, however, guaranteed by the *Canadian Charter*, although this notion was developed in *Canada (Commission des droits de la personne)* c. *Taylor*[106]. As dignity and reputation are closely correlated, it would be important to mention that the notion of reputation also exists in Quebec in section 4 of the *Quebec Charter of Rights and Freedom* and in the *Civil Code of Quebec* under sections 3[107] and 35[108]. Furthermore, we see the notion of dignity appear in international law. Without enumerating an exhaustive list, this notion appears in the *Universal Declaration of Human Rights*[109] in the first and fifth paragraphs. It is brought back in the preamble of the *International Covenant on Civil and Political Rights*[110]. Moreover, we see it again in the preamble of the *International Covenant on Economic, Social and Cultural Rights*[111].

---

[104] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 83.

[105] *Charte des droits et libertés de la personne*, RLRQ, c. C-12. In fact, personal information protection laws convey a moral content, that of "human dignity and self-development" […], K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 47.

[106] "[…] That the values of equality and multiculturalism are enshrined in ss. 15 and 27 of the *Charter* further magnify the weightiness of Parliament's objective in enacting s. 13(1). These *Charter* provisions indicate that the guiding principles in undertaking the s. 1 inquiry include respect and concern for the dignity and equality of the individual and a recognition that one's concept of self may in large part be a function of membership in a particular cultural group. As the harm flowing from hate propaganda works in opposition to these linchpin *Charter* principles, the importance of taking steps to limit its pernicious effects becomes manifest", *Canada (human Rights Commission)* v. *Taylor*, [1990] 3 SCR 892, 1990 CanLII 26 (SCC).

[107] "3. Every person is the holder of personality rights, such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy. […]."

[108] "35. Every person has a right to the respect of his reputation and privacy.
The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law."

[109] "Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,
(…)
Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom […]", *Universal Declaration of Human Rights*, res. 217A (Ill), Off. doc., U.N.G.A., 3rd Sess., Supp. No. 13 at 71, U.N. Doc. A/810 (10 December 1948).

[110] "Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,
Recognizing that these rights derive from the inherent dignity of the human person, […]".

In the European Union, the first article of the *Charter of Fundamental Rights of the European Union* states that "Human dignity is inviolable. It must be respected and protected".

What all these laws have in common is that they set the right to dignity as a foundation of human rights and freedom[112]. Such is the case with the *Quebec Charter* where it states in the second and third paragraphs of the preamble:

> "Whereas all human beings are equal in worth and dignity, and are entitled to equal protection of the law;
>
> Whereas respect for the dignity of human beings, equality of women and men, and recognition of their rights and freedoms constitute the foundation of justice, liberty and peace […]".

Nonetheless, while the right to dignity is guaranteed in these legal instruments, the definition of dignity is not defined in any of them[113]. What we know is that amongst many things, human dignity has been linked to public image and reputation[114], such as was the case in *Corriveau* c. *Canoe Inc*.[115]. Dignity must also be protected from "unwarranted government intrusions" in the intimate sphere of a person's life[116]. Therefore, because of the vast array of information accessible on a person through some smart devices, something such as a false accusation based on the data retrieved on a personal smart device could infringe on the dignity of the accused; this is if the accused has suffered damage to their reputation. This would be considered as defamation

---

International Covenant on Civil and Political Rights, 16 December 1966, 999 U.N.T.S. 171 (came into force in Canada on 19 May 1976 and ratified by Québec on 1 November 1978).

[111] "Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,
Recognizing that these rights derive from the inherent dignity of the human person, […]", *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, 993 U.N.T.S. 3 (came into force in Canada on 19 August 1976 and ratified by Québec on 21 April 1976).

[112] Henk BOTHA, "Human dignity in comparative perspective", (2009) 20 *Stellenbosch L. Rev*. 171.

[113] Christian BRUNELLE, "La dignité dans la Charte des droits et libertés de la personne : de l'ubiquité à l'ambiguïté d'une notion fondamentale", (2006) 66.5 *R. du B*. 143, on page 147; *Commission des droits de la personne et des droits de la jeunesse (Succession Duhaime)* c. *Satgé*, 2016 QCTDP 12 (CanLII).

[114] Maxine GOODMAN, "Human Dignity in Supreme Court Constitutional Jurisprudence", (2006) 84 *Nebraska Law Review* 741, p. 758.

[115] *Corriveau* c. *Canoe inc*., 2010 QCCS 3396 (CanLII).

[116] Giorgio RESTA, "Human Dignity*", McGill Companion to Law*, June 2015, online: <https://www.mcgill.ca/companion/list/human-dignity> (consulted on January 21, 2020).

of character. To establish civil liability for this action, the victim of defamation would have to prove the existence of an injury, a wrongful act and a causal connection between the two, such as it was intended by section 1457 of the *Civil Code of Quebec*. Moreover, because of the number of information revealed about users from smart health devices, as we shall see later on, this could lead to a form of discrimination under the ground of physical disability of section 15 (1) of the *Canadian Charter* or similarly to a discrimination under section 10 of the *Charter of human rights and freedoms* under the ground of handicap[117]. Thus, an individual is faced with discrimination when they are denied of their intrinsic worth, therefore violating their right to dignity and equality simultaneously[118]. The violation of one's dignity can also come from something as simple as exposing publically personal information that can interfere with a user's reputation, especially if it infringes on a person's reasonable expectation of privacy. If the information was gathered without proper consent and had a negative impact on the user's reputation, there will be a double violation: a violation of one's privacy and of dignity. Preserving one's dignity is therefore a key element in accessing information about a user of smart technologies and should be taken into consideration with other key components that might impact a user negatively, such as race and health.

This being said, knowing how we give away our rights, how they can be taken away from us and what is left of them raises questions regarding our personal sensitive information such as our health data. Although the usual way to share it is through a physician and a patient, the rise of technology allows for other types of sharing and gathering of our information, mainly online and with the use of smart health devices such as pacemakers, Fitbits and cellphone health applications. Indeed, the information gathered by brands such as Apple and Android have software platforms with systems[119] that support third-party developers which in turn get access to our data. These platforms allow for this data to be collected and shared by devices of the same brand. An Apple user will have access to Apple Health. If an Apple user also has a Fitbit, its information will be shared between the smart wristband and the cellular device. Android users

---

[117] *Charte des droits et libertés de la personne,* prev. cited, note 105.
[118] Giorgio RESTA, "Human Dignity", prev. cited, note 116.
[119] "(apps, dashboards, SDKs (Software Development Kits) and REST APIs (RE presentational State Transfer Application Programming Interfaces)", Francisco de ARRIBA-PÉREZ, Manuel CAEIRO-RODRIGUEZ and Juan M. SANTOS-GAGO, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", (2016) 16 *Sensors (Basel)* 1538, point 2.1. online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/> (accessed on October 20, 2019).

have a similar application called S-Health which supports all wearable devices. In order to use these applications, these devices use sensors able to monitor the Heart Rate (HR) and any movement generated by the users[120]. As a matter of fact, our location and our movements[121] are the most commonly recorder personal data. With the amount of data constantly recorded, kept and perhaps even shared by developers, there is little place for our right to privacy. Moreover, some smart device companies admit to keeping our information and to be willing to share it if need be. Such is the case with Fitbit that admits in its Privacy Policy to keeping "information about [their users] and [their] use of the Services for as long as necessary for [Fitbit's] legitimate business interests, for legal reasons, and to prevent harm, […]"[122]. We have seen what keeping information for a longer than necessary time has led to[123]. We already know what could happen to personal information in scandals regarding Ashley Madison[124], Equifax[125] and Uber[126] data breaches, just to name a few. If it has become more convenient to use smart health devices to monitor one's health, it also comes with its own risks; a data breach being a non-zero probability.

Beyond the fact that personal information could be seen by the public, there is a stronger risk that it could be collected and used by third parties through smart health technologies; such is the case of some smart thermometers[127]. Kinsa thermometers can be connected to a smartphone and generate a person's temperature within seconds[128]. Its application holds a journal which records each entry and patients' symptoms while providing feedback. However, this short term

---

[120] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119, point 2.3.

[121] We consider personal information to be any movement that might reveal a person's geolocation, amongst other identifiable information; however, we acknowledge that any movement recorded could reveal sensitive information, such as the one performed behind closed doors.

[122] FITBIT, "Fitbit Privacy Policy", September 18, 2018, online: <https://www.fitbit.com/en-ca/legal/privacy-policy> (accessed on March 24, 2019).

[123] *Report of an Investigation into the Security, Collection […]*, prev. cited, note 82.

[124] Zak DOFFMAN, "Ashley Madison Has Signed 30 Million Cheating Spouses. Again. Has Anything Changed?", *FORBES*, August 23, 2019, online: <https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-million-cheating-spouses-signed-since-the-hack/#271a8d803878> (consulted on October 18, 2019).

[125] REUTERS, "Equifax to pay up to $700 million in US data breach settlement", *CNBC*, July 22, 2019, online: <https://www.cnbc.com/2019/07/22/equifax-to-pay-up-to-650-million-in-data-breach-settlement.html> (consulted on October 18, 2019).

[126] Sara SALINAS, "Uber will pay $148 million in connection with a 2016 data breach and cover-up", *CNBC*, September 26, 2018, online: <https://www.cnbc.com/2018/09/26/uber-to-pay-148-million-for-2016-data-breach-and-cover-up.html> (consulted on October 18, 2019).

[127] TVA NOUVELLES, "Des thermomètres intelligents jugés trop indiscrets", October 24, 2018, online : <https://www.tvanouvelles.ca/2018/10/24/des-thermometres-intelligents-juges-trop-indiscrets> (accessed on October 18, 2019).

[128] KINSA, "Which Kinsa Thermometer is best for me? ", online: <https://www.kinsahealth.com/teladoc/products> (consulted on October 20, 2019).

convenience comes at a cost; the one of sharing personal health information with the brand. This smart device is one of the many that stores a user's geolocation amongst many other personal data without the knowledge of the latter. The data gathered is used to cater specific publicity to the users, meaning their personal information might have been sold and sent to other third parties[129]. The widespread of personal information therefore puts the users at risk of it being disclosed. Although this specific brand certifies that it keeps all data anonymous, retracing data to its owner could be done, and by some without much difficulty. More so, as we now know, as much as our laws protect personally identifiable information, there are still no laws specifically protecting anonymous information. Yet, another problem is if these companies who sell smart health devices are located in the U.S. or have an affiliation with the United States, in which case such data can be accessed through different judicial means, amongst others.

Furthermore, as smart technologies emerge, we are increasing the exposure of our personal information to other governments. As a matter of fact, in recent years, there has been an increase in wearable technology such as: "fitness trackers, smart watches, connected headsets, smart glasses, wrist bands"[130] and so much more. These devices can gather information on our vital signs such as our heart rate and our skin temperature and compute our movements as well. This is possible due to the fact that these devices use multimodal learning analytics which grab a variety of information through "audio, video, location, motion, temperature, humidity or luminosity data, among others"[131]. A legitimate concern may then arise as to who precisely has access to this information. As a matter of fact, China is just one example of a country storing information from the West through different smart technologies. As an example, there is a recent controversy that surrounds the Nokia 7 Plus phones[132]. HMD Global had been accused of sending personal data of the phone's users to China and admits to such a mistake which resulted in the transfer of personal information to third parties in China. Nonetheless, it denies that the latter were able to process such information and identify users through it. Moreover, the Chinese phone company Huawei was also under scrutiny for spying on the West. FBI Director

[129] KINSA, "Kinsa's Privacy Principle", online: <https://www.kinsahealth.co/privacy-principles/> (consulted on March 19, 2020).
[130] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119.
[131] *Id*.
[132] NOKIA, "HMD Demystifies Reports About Data Breaches, Spying ECT. On Nokia Phones", *NOKIAMOB*, March 22, 2019, online: <https://nokiamob.net/2019/03/22/hmd-demystifies-reports-about-data-breaches-spying-etc-on-nokia-phones/> (accessed on March 27, 2019).

Christopher WRAY even said that the use of the company's equipment could enable Beijing to "maliciously modify or steal information, conduct undetected espionage, or exert pressure or control"[133]. These are only two brief examples of data breaches performed by advanced phone companies. Besides, while our information can be taken and possibly used against us by foreign governments, a greater worry is that our own information can be used against us in our country.

c) Smart Devices Turning Against Their Owners

With electronic devices being permitted into evidence, as we shall see below, it is only a matter of time until smart health devices are granted such entry. Following a warrant, law enforcement officers can get a hold on someone's private information regarding their health if such information can play a role in solving a specific case. Thus, disclosure of health data[134] and the violation of a right to privacy are potential risks associated with the use of smart devices able to monitor users' health. This potential mass surveillance could also affect the activities of users, potentially breaching articles 7 and 8 of the *Canadian Charter of Rights and Freedom*, mainly violating a person's right to liberty and against unreasonable search and seizure[135], thus unreasonable invasions of privacy.

It is also important to note that in some cases, seizure of a personal device, following a lawful arrest, has been permitted and did not violate section 8 of the Charter as long as the search was properly documented and served the purpose related to the arrest[136]. On the other side, if the search of a device was unlawful and evidence was found following it, section 24 (2) of the Charter requires that the evidence be excluded from trial, but we see that this is not always the case[137]. Indeed, in contrast to the United States where illegally obtained evidence will defeat the investigation, even considering the administration of justice, in Canada, when evidence is obtained illegally, it will be a question of assessing the impact on the administration of justice[138]. This means that there is no insurance towards personal data being fully protected from use in

---

[133] Nathan VANDERKLIPPE, "Top Huawei executive says not even Xi Jinping could compel it to help China spy in other countries", *THE GLOBE AND MAIL*, March 26, 2019, online: <https://www.theglobeandmail.com/world/article-top-huawei-executive-says-not-even-xi-jinping-could-compel-it-to-help/> (accessed on March 27, 2019).
[134] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98.
[135] *Charte canadienne des droits et libertés,* prev. cited, note 33, articles 7 and 8.
[136] *R.* v. *Fearon*, [2014] 3 SCR 621, 2014 SCC 77 (CanLII).
[137] *R.* v. *Vu*, [2013] 3 SCR 657, 2013 SCC 60 (CanLII).
[138] Clause LAFERRIÈRE, *États-Unis d'Amérique/Canada : Traité de droit de la sécurité nationale*, Montréal, Wilson & Lafleur ltée, 2018, 1081 pages, on page 930, para. 3643-3646.

courts. Furthermore, mobile phones and personal computers[139] are not immune from being searched; considering this, the same could apply to other technological devices that keep track of our personal data such as smart health devices.

In fact, if we consider the *R*. v. *Kang-Brown*[140] case, some of the judges concluded that odor, from a bag, is not something our right to privacy covers. This is interesting because the seizure of a personal item, a bag, which emitted an odor from carrying drugs, did not infringe on the defendant's right to privacy, even if that seizure was clearly unlawful and not warranted. Although the judges had differing opinions on this matter, it simply shows that cues perceived by law enforcement officers could lead to an unwarranted search. If the latter are ever able to analyze and gather data emitting from our smart health devices, they could search a user based on his heart rate in a highly secured area such as an airport. Thus, a false accusation could impact the dignity of a person, especially if the public opinion is detrimental to their profession[141].

Moreover, smart devices could equally be used against individuals. As one might imagine, there are always pro's and con's to everything. In the cases we will see later in the thesis, smart devices benefited their owners by serving as additional evidence in a murder trial. There are however cases where such devices can turn against their owners. This has been the case with tracking devices in *R.* v *Wise*[142], electricity consumption records in *R*. v. *Plant*[143] and *R.* v. *Gomboc*[144], the use of infrared technology to detect heat patterns in homes in *R*. v. *Tessling*[145], the seizure of a personal computer in relation to child pornography in *R*. v. *Morelli*[146] or a laptop in *R.* v *Cole*[147] and even the seizure of cellphones to reveal incriminating text messages in *R.* v. *Fearon*[148], in *R.* v. *Marakah*[149] and in *R*. v. *Jones*[150]. What all of these cases have in common, is the use of smart technology used to incriminate someone. Indeed, smart technology, whether it is

[139] *Laushway* v. *Messervey*, 2014 NSCA 7 (CanLII).
[140] *R*. c. *Kang-Brown*, [2008] 1 SCR 456, 2008 SCC 18 (CanLII).
[141] *Corriveau* c. *Canoe inc*., 2010 QCCS 3396 (CanLII).
[142] *R.* v. *Wise,* [1992] 1 SCR 527, 1992 CanLII 125 (SCC).
[143] *R.* v. *Plant*, [1993] 3 SCR 281, 1993 CanLII 70 (SCC).
[144] *R.* v. *Gomboc,* [2010] 3 SCR 211, 2010 SCC 55 (CanLII).
[145] *R*. v. *Tessling*, [2004] 3 SCR 432, 2004 SCC 67 (CanLII).
[146] *R*. v. Morelli, [2010] 1 SCR 253, 2010 SCC 8 (CanLII).
[147] *R.* v. *Cole,* [2012] 3 SCR 34, 2012 SCC 53 (CanLII).
[148] *R.* v. *Fearon,* [2014] 3 SCR 621, 2014 SCC 77 (CanLII).
[149] *R.* v. *Marakah,* [2017] 2 SCR 608, 2017 SCC 59 (CanLII).
[150] *R.* v. *Jones,* [2017] 2 SCR 696, 2017 SCC 60 (CanLII).

advanced or not, can compute or retrieve data from an individual without their awareness. This is also the case with smart health devices. The data they compute can reveal the user's location similarly to tracking devices on other smart technology along with more sensitive data generated by search queries or any interaction with the device. Thus, it is equally important to address the risks generated by smart devices as such risks are likely to reappear in smart health devices.

Another case pertaining to the use of technology to incriminate a defendant was seen in Canada, in *Garderie Les << Chat >> ouilleux inc*. et *Marchese*[151]*,* which is one of many similar cases. While a daycare teacher was claiming damage benefits from a quite severe work-related injury, photographs produced at the hearing, posted on "Facebook", portrayed her on vacation in the Dominican Republic in positions that were not compatible with the injury she alleged to have[152]. This, amongst other things, reduced her credibility in her testimony which led to a dismissal of her injury allegations. Who is to say that the GPS feature on one's smart health device cannot fulfill the same purpose? Had the pictures been taken on a smart device, it would also have been possible to use the metadata generated by it to prove the date and the location of when the pictures had been taken. Moreover, someone can take a sick leave, but simply by using their smart health device, they can send out data about their location and their whereabouts, essentially compromising them from the simple use of their device. This could be applicable to other smart devices as well. For example, by using the application called "Snapchat", available on many devices with a camera, it is possible to see where a user is exactly in the world and pinpoint their exact location, if the sharing location option has not been disabled. Facebook has a similar feature that allows seeing who amongst your friends are nearby[153]. This means that if any smart heath device has similar applications with geolocation features, other users might track you down. This particular issue has not yet been addressed by the Privacy Commissioner of Canada.

---

[151] *Garderie Les << Chat >> ouilleux inc*. et *Marchese*, 2009 QCCLP 7139 (CanLII).
To note that many more cases exist resembling this one such as *Syndicat des Enseignant(e)s de Charlevoix* v. *CS de Charlevoix*, 2014 CanLII 50053 (QC SAT) and *Syndicat canadien de la fonction publique (FTQ, section locale 3535)* c. *Société des alcools du Québec (Logistique & distribution)*, 2011 CanLII 84831 (QC SAT).
[152] *Garderie Les << Chat >> ouilleux inc*. et *Marchese*, *Ibid*., par. 59.
[153] Geoffrey WHITE, *Off the Grid: Pinpointing Location-based Technologies and the Law*, PUBLIC INTEREST ADVOCACY CENTRE, June 2015, p. 28, online: <http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report.pdf> (consulted on March 27, 2020).

Furthermore, if it is not the Government, third parties or regular individuals collecting personal data, then we can be assured that these smart devices do so themselves. In fact, wearable healthcare technology is specifically designed to collect data of its user's personal health[154].

Whatever the scenario, smart devices, including smart health devices, are no longer just utility gadgets and can turn against their owners. Nonetheless, the risks are not just limited to the users of smart health devices.

2. Risks for the Government in Establishing a National Database

There are numerous risks for users of smart health devices associated with the usage of these devices and the storing of their personal health data. These risks could make us doubt the viability of a database solution, which is why it is important to address them. Additionally, there are also risks for the Government in pursuing our solution. The Canadian Government ought to be careful when accessing and allowing the sharing of personal information about its citizens as our fundamental rights, in particular the right to freedom and to privacy, are supreme rights located in the *Canadian Charter of Rights and Freedom*. Such rights can only be limited by section 1 of the *Canadian Charter*"[155]. The right to privacy in particular is to Canadians "not just […] an individual right, but […] part of our social or collective value system". It is a "fundamental right to human dignity and integrity, to one's honour and reputation". Indeed, "privacy is vital to an individual's dignity, autonomy, and personal growth". In fact,

> "Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others—either with trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity"[156].

---

[154] Alicia PHANEUF, "Latest trends in medical monitoring devices […]", prev. cited, note 9.
[155] "I. The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".
[156] HOUSE OF COMMONS STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF PERSONS WITH DISABILITIES, *Privacy: Where do we Draw the Line?*, April 1997, p. 6, online: <https://www.priv.gc.ca/media/1314/02_06_03d_e.pdf> (consulted on March 27, 2020).

Yet, a more recent report from the Office of the Privacy Commissioner of Canada shows that the vast majority of Canadians (92%) "expressed some level of concern about the protection of their privacy"[157]. They do nonetheless feel more confident that "the federal government respects their privacy rights" more than businesses[158]. This gives hope that Canadians would entrust their data in the hands of the Canadian Government were it to implement a national database.

Nonetheless, some risks persist and need to be addressed for this confidence not to dissipate and for citizens' right to privacy not to be breached; risks that may be out of the hands of the Canadian Government or harder to control and mitigate.

a) Hacking of Personal Information

If health information can be seized via legal means, it can also be stolen through ransomware. Thus, a national database generated by smart health devices can indeed be prone to hacking just as any other health database, computer or server. In fact, as an example, this has already been done using the ransomware called WannaCry that found a vulnerability in Microsoft[159]. It affected numerous computers in over 150 countries, encrypting their files, and demanding that the users of the computers pay in Cryptocurrency[160] to unlock their files[161]. Before the payment is done, it is usually impossible to regain access to the encrypted files, unless a kill switch is found for the malware. This malware is often delivered through emails and is

---

Also see: OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy", 2019, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/> (accessed on May 18, 2020).
Also see: K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 47.

[157] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "2018-19 Survey of Canadians on Privacy: Final Report", online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/> (consulted on March 27, 2020).

[158] *Id*.

[159] Josh FRUHLINGER, "What is WannaCry ransomware, how does it infect, and who was responsible?", *CSO*, August 30, 2018, online: <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> (consulted on March 19, 2020).

[160] There are many Cryptocurrency systems such as Bitcoin, Litecoin, Peercoin, Ethereum, Ripple, Namecoin, Auroracoin, Blackcoin, Dash, Decred, and Permacoin, amongst others. A Cryptocurrency is essentially "a peer-to-peer digital exchange system in which cryptography is used to generate and distribute currency units".
Ujan MUKHOPADHYAY, Anthony SKJELLUM, Oluwakemi HAMBOLU, Jon OAKLEY, Lu YU, and Richard BROOKS, "A brief survey of Cryptocurrency systems", (2016) *14th Annual Conference on Privacy, Security and Trust (PST)* 745.

[161] Zack WHITTAKER, "Two years after WannaCry, a million computers remain at risk", *TECHCRUNCH*, May 12, 2019, online: <https://techcrunch.com/2019/05/12/wannacry-two-years-on/> (consulted on March 20, 2020).

released once the recipient opens the email; this is also known as a phishing scam[162]. Nevertheless, because of the illegal nature of this activity, there is no guarantee that once the payment goes through, that access to the files will be granted.

This incident affected hospitals in the United Kingdom and high-profile systems in Britain's National Health Service, Government systems, railway networks and even private companies. The hospital staff was forced to work with pens and paper but could not use the affected medical systems. Surgeries and appointments had to be canceled due to the ransomware blocking access to doctor's computers, demanding payment to restore access[163].

Yet, other malware such as WannaCry exist, namely Upatre, Cerber, Emotet, Locky, Petya, Ramnit, Fareit, PolyRansom, and Terdot/Zloader and they are affecting healthcare the most through ransomware[164]. These attacks are able to change a patient's data, hijack medical devices and can even shut down an entire hospital[165]. This is done until the ransomware is paid. Similarly to WannaCry, NotPetya caused $10 billion in damage to companies and users of computers around the world and affected thousands of health care delivery organizations which were left unable to use their programs[166].

These two incidents are used as examples to demonstrate the severity of the concern. Moreover, healthcare generally is an easy target for malware attacks and hackers interested in stealing personally identifiable information are increasing their attacks in this field. Indeed, *The State of Healthcare Cybersecurity* report has shown a 60% increase in 2019 of threat detections coming from healthcare organizations[167]. This is in part due to the fact that medical institutions allocate their budget to research, patient care and to new technology but cybersecurity often comes

---

[162] Chris GRAHAM, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history", *THE TELEGRAPH*, May 20, 2017, online: <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/?subId3=xid:fr1584728850959jff> (consulted on March 20, 2020).
[163] *Id*.
[164] Fred DONOVAN, "Healthcare Industry Takes Brunt of Ransomware Attacks", *HEALTHITSECURITY*, May 3, 2018, online: <https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks> (consulted on March 20, 2020).
[165] Nicole WESTMAN, "Health Care's Huge Cybersecurity Problem", *THE VERGE*, April 4, 2019, online: <https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation> (consulted on March 20, 2020).
[166] *Id*.
[167] CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", November 2019, p. 5, online: <https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf>.

second. As well, the medical sector was ranked as the seventh-most targeted industry and malware detections in this industry rose by 45%[168]. The healthcare industry is mostly affected by Trojan malware which increased by 82%; the most common ones are Emotet and TrickBot. The latter is the number one threat in healthcare today.

The methods currently used for cybercriminals that seek to penetrate healthcare networks are to compromise vulnerabilities in third-party vendor software that have not been tackled and use phishing scams through malicious emails, attachments and links. Such vulnerabilities can be found in smart health devices. In addition, one of the reasons for targeting healthcare specifically is due to their large databases which contain personally identifiable information and give access to other devices connected to the network. The sensitive information accessed by cybercriminals gives them a high return on investment. More precisely, they are interested in "complete name, date of birth, family relations, Social Security Number (SSN), addresses, credentials, driver's license numbers, email addresses, phone numbers, and […] sensitive data related to health that includes health conditions, scans or medical imaging results, blood test results, family and/or genetic history, case history, drug prescriptions, scheduled appointments, food allergies, physicians' diagnoses, notes, and other observations. Such data is rarely found elsewhere"[169]. Personal health data is then possibly sold on the Dark Web and could generate ten times more revenue than normal personally identifiable information[170]. In fact, a partial electronic health record (EHR) could sell for $50 while a credit card number could be worth $1[171]. This said, as we have seen earlier on, hackers could just as well hack into smart health devices through Wi-Fi or other means and access user PHI. The information generated by smart health devices can be just as lucrative or more as such devices can open the door to other data, namely finances.

Along with the possibility of selling the information, hackers could use the data stolen to commit fraud and identity theft. Doing so is indeed possible through the information gathered by malicious health applications on smart devices[172], some of which are found on smart health

---

[168] CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", prev. cited, note 167, p. 4.
[169] *Id*., p. 22.
[170] *Id*., p. 22-23.
[171] *Id*., p. 23.
[172] Danny PALMER, "Mobile security: These health apps aren't good for your phone or your privacy", *ZDNET*, October 7, 2019, online: <https://www.zdnet.com/article/mobile-security-these-health-apps-arent-good-for-your-phone-or-your-privacy/> (consulted on March 20, 2020).

devices or connected to the latter, or by purchasing the information on the Dark Web. With this illegally obtained information, criminals can assume the identities of real patients and "buy medical equipment, prescription drugs, or undergo expensive medical services under their victims' names"[173]. Moreover, the theft of personally identifiable health information is made easier through the Internet of Things (IoT). Having a great magnitude of connected smart devices means they are more likely to get infected and a higher infection rate would make them more susceptible to malware[174]. Hence, having a smart health device connected to other smart devices can increase a user's vulnerability to a data breach. Furthermore, having apps generate sensitive health information could mean higher chances of data leakage[175] and a greater possibility of hacking through vulnerabilities within the applications.

Thus, creating a national and international database generated by smart health devices could become an open invitation for cybercriminals to hack into the personal data of Canadians. The Government should therefore find ways to mitigate hacking risks to avoid that citizens' PHI data is accessed without consent, whether through a national database or through their wearables. Yet, apart from the previously mentioned concerns, the solution itself does not come without flaws.

b) Efficiency and Flaws of the System

While the advantages of having live inputs constantly generated by smart health devices can be tremendously beneficial on an individual level, analyzing the inputs of smart technologies to report on the health condition of a population might have its complications. This is where the importance of laws and regulations comes in. This project should take into account national and international laws on the protection of personal information while also respecting the terms and conditions of partnering private entities such as Apple that requires, as we shall see, that the data be encrypted, not be sold to third parties and that the users be informed of how their data was used. As with any information, the users would be able to withdraw at anytime and cease sharing their personal health data when they desire. However, protecting personal data this way could hinder the process of gathering accurately health statistics.

---

[173] CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", prev. cited, note 167, p. 24.
[174] *Id*., p. 24.
[175] *Id*., p. 30-31.

Furthermore, there are some problems that could arise with using smart health devices as a tool in healthcare. We shall list a few of them to give us a general idea of what we should expect or can encounter.

- **The first problem** would come from not having a large enough sample size to be able to accurately represent what is happening in a population at a certain period of time. In addition, the most obvious problem would come from the lack of participation of people from different ethnical groups, social classes, regions and countries. As we will soon see, for something to be considered an epidemic, it requires that the number of cases reported be higher than usual in a population. Yet, if the sample size is too small, getting this data could prove to be difficult unless the data generated by smart health devices is used in combination with other data, such as Google search queries, media reports, surveys, access to purchased medication and more[176]. Nonetheless, creating such a database would not be useful if only middle-class and above citizens are able and willing to opt-in to this idea. Due to their ability to live healthier lives than the less fortunate[177], health data generated by these users would skew the overall health results and perhaps even turn us away from important health problems arising in a country, and currently, "it is the wealthiest adults who are current users of smart devices"[178].

- **The second problem** comes from the right of an individual to stop sharing personal data at any time. While having live inputs can prove to be effective in spotting and differentiating viruses from colds, amongst other things, if the data gets cut off in the middle of such analysis, the whole premise of the research becomes flawed as the analysis would cease the moment the user stops sharing their data and it would impact the

[176] Mauricio SANTILLANA, André T. NGUYEN, Mark DREDZE, Michael J. PAUL, Elaine O. NSOESIE, John S. BROWNSTEIN, "Combining Search, Social Media, and Traditional Data Sources to Improve Influenza Surveillance", prev. cited, note 13.
[177] Heather MURPHY, "Rich People Don't Just Live Longer. They Also Get More Healthy Years", *THE NEW YORK TIMES*, January 16, 2020, online: <https://www.nytimes.com/2020/01/16/science/rich-people-longer-life-study.html> (consulted on February 17, 2020); Paola ZANINOTTO, George David BATTY, Sari STENHOLM, Ichiro KAWACHI, Martin HYDE, Marcel GOLDBERG, Hugo WESTERLUND, Jussi VAHTERA and Jenny HEAD, "Socioeconomic Inequalities in Disability-free Life Expectancy in Older People from England and the United States: A Cross-national Population-Based Study", (2020) XX *Journals of Gerontology: Medical Sciences*, online: <https://academic.oup.com/biomedgerontology/advance-article/doi/10.1093/gerona/glz266/5698372>; Guy PARÉ and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 41.
[178] Heather MURPHY, "Rich People Don't Just Live Longer. They Also Get More Healthy Years", *Id*.

overall study. This could however keep working if the sample size is big enough to account for the people that will stop sharing their information over time. Nonetheless, due to the fact that the data would be extracted in an anonymous way and because the users would have the right to cease sharing their information at any time, the information analyzed would not be a perfect representation of what is happening. This brings us to our third problem.

- **The third problem** comes from false positives. While smart health technologies have been proven to be very effective at detecting health problems early on, the information they gather can create false positives and if analyzed separately from all other available data, this could waste important national resources. Fitbit's, for example, count the number of steps taken in a day. Knowing how many steps a population takes can show activity levels of a society and detect a potential health change through a decreased amount of steps. If more people are taking fewer steps and if they are also experiencing an increased heart rate that could signify that flu or a virus is on the way. Yet, external conditions could cause a Fitbit to generate more or fewer steps. Indeed, it would be important to consider additional factors that can influence a person's sensory outputs. Anything ranging from seasonal trends, a change in profession, holidays, the weather, abnormal temperature deviations, to an increase in stress factors, all of which can influence the data which can be mistaken for a virus. More so, if a set amount of people develop flu-like symptoms, it may signal the presence of the flu or something else altogether. Furthermore, any external factor such as an increase in weight, alcohol consumption and stress could also increase a person's susceptibility to an infection. Hence, this is why it would be important to take into consideration external factors when monitoring infectious diseases. People's level of activity by season should also be taken into account, meaning if the data is retrieved during the winter season, people's level of activity could be diminished which can result in an increased heart rate due to deconditioning. Comparing the data to the average physiological results of a population could be efficient in monitoring the start and spread of a disease[179]. What these smart

[179] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, "Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based

devices do not do, is take external conditions into consideration when generating data from their user. The main worry would be to cause unnecessary alarms in a population and to waste important resources on problems that are not of public health concern.

- **The fourth problem** is internet connectivity and device availability. Although it is becoming less and less of a problem with internet networks getting a larger coverage, real time data analysis would not be able to be performed unless the users of smart health devices are connected to the internet. Usually, the smart device searches for an Internet connection, and when it has been established, sends the data collected to the server. Wearables might still collect data without an Internet connection but will not send the data unless a connection is established[180]. This said, while the data generated by smart health devices could reach the national and international database in its own time, it could be harder to generate live feeds from these devices if the users are not constantly connected to the Internet. On a similar note, another problem that can be seen is that although smart health devices have a grand number of sensors such as: heart rate, accelerometer, pedometer, walking speed, calorie intake, distance, gyroscope, magnetometer, barometer, altimeter, GPS, ambient light, thermometer, ultraviolet light sensor, galvanometer, microphone and analytics sleep[181], each of them only has a few of the ones listed above and they do not always have the same ones. If a big percentage of the population solely used the Fitbit, then it would be practically impossible to compute other data such as the walking speed which is available in the Microsoft band. It would then become important to have data generated from a variety of smart heath devices to have the most accurate representation of a population's overall health.

Perhaps another worry with the use of smart devices is the potential access of users' data by Government agencies. If Amazon, Google or Apple, as an example, were to give away personally identifiable information to the Government, the users would lose trust in these brands

---

study", (2020) 2 *THE LANCET DIGITAL HEALTH*, online: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30222-5/fulltext> (accessed on May 1, 2020).

[180] Francisco de ARRIBA-PÉREZ, Manuel CAEIRO-RODRIGUEZ and Juan M. SANTOS-GAGO, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", prev. cited, note 119, point 3.2.1., Link 2.

[181] *Id*., point 5.1.1., Table 4.

and cease the purchase of their products[182]. This is why it would be very important keep users' data anonymous if shared with a national and international database, to ensure that privacy and trust are not lost throughout the process.

In essence, there are individual risks to using smart health devices, mainly the risk of personal information being collected with or without consent and used against the users or against the Government such as when confidential data is hacked through ransomware. However, there are also risks in computing the data generated by wearables to enhance public health surveillance as it may create misinformation due to the flaws mentioned above. Yet, despite the latter, smart devices that are turning towards health are getting more advanced by the year and can prove to be an asset in evaluating national and international health problems. As an example, Apple Series 4 watch, which was released in September 2018, has cell phone connectivity, GPS, acceleration sensors, a pulse rate sensor and ECG electrodes; as of December 6th 2018, Apple had released an app capable of analyzing ECG and atrial fibrillation (AF) in the users[183]. The range of sensors in this device can generate crucial data which could enhance the monitoring of diseases. As we will see in the following sections, the advantages of smart devices can outweigh the potential risks.

B. The Case for Using Smart Health Devices Individually and Collectively

Considering solely the risks mentioned previously, it may seem as though the use of smart devices is to be cautioned, reduced or even avoided. While that may indeed diminish the risks of a violation of one's right to privacy, the true potential of smart health devices is yet to be exhausted. Certainly, as we will now demonstrate, smart health devices have their fair share of benefits which, as argued, may outweigh the costs. Indeed, both the Government and the general population can benefit from the data extracted from such devices as they have the potential of improving healthcare and patient care, preventing diseases or viruses and enhancing the safety and security of a country. Additionally to proving the latter, we will demonstrate the feasibility of using these devices in the public health sector and the extent of their potential so far.

---

[182] Sonia RAO, "In today's homes, consumers are willing to sacrifice privacy for convenience", *THE WASHINGTON POST*, September 12, 2018, online: <https://www.washingtonpost.com/lifestyle/style/in-todays-homes-consumers-are-willing-to-sacrifice-privacy-for-convenience/2018/09/11/5f951b4a-a241-11e8-93e3-24d1703d2a7a_story.html> (accessed on April 29, 2020).

[183] Kenneth R. FOSTER and John TOROUS, "The Opportunity and Obstacles for Smartwatches and Wearable Sensors", (2004) 10 *IEEE Pulse* 22, online: <https://ieeexplore.ieee.org/abstract/document/8666099>.

1. Our Information in the Hands of the Government

While there are a number of risks in increasing the amount of health information available to the Government, there are undeniable benefits to sharing our personal health data with the latter, such as having access to a vast array of data on its population, catering accordingly its services, allowing for more funding in certain designated fields, and making policies which benefit a society as a whole[184]. As an example, in Scandinavian countries, in order to offer better services to the population, access to personal data is more than welcomed because the Government can effectively think on behalf of its people as it knows what its population's needs are[185]. As well, it may seem that the Government's interest revolves more in the community than in individual interests of people, meaning it may use individual information to make policies benefiting the society to the detriment of some individuals' privacy. The benefits of breaching the privacy of some could be of a significant help to a community at large. If we take healthcare for example and the prevention of certain diseases or their outbreaks, the data we input on different search engines can help the Government stop or prevent a future health crisis by getting access to the common trends that are searched within a certain amount of time and at a certain location[186].

In any case, smart health devices have the potential of offering benefits both to the Government and to its population. Nowadays, the use of Remote Biosensing Technologies (RBT) in healthcare and in law has become increasingly popular as they are likely to reduce costs while improving health outcomes[187]. Indeed, data gathered by smart health devices plays a "key role in aiding health systems to reduce costs, improve quality, identify populations at risk, connect with consumers and better understand performance"[188]. In addition, smart health devices turning to healthcare have not only successfully improved health services but they have also effectively

---

[184] Jeroen VAN DEN HOVEN, "Information Technology, Privacy, and the Protection of Personal Data", prev. cited, note 73, p. 304.
[185] *Id*.
[186] Madhur VERMA, Kamal KISHORE, Mukesh KUMAR, Aparajita RAVI SONDH, Gaurav AGGARWAL, Soundappan KATHIRVEL, "Google Search Trends Predicting Disease Outbreaks: An Analysis from India", (2018) 24 *Healthc Inform Res* 300.
[187] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies in Healthcare and the Law", prev. cited, note 98, on page 61.
[188] DELOITTE CENTRE FOR HEALTH SOLUTIONS, "Medtech and the Internet of Medical Things | How connected medical devices are transforming health care", July 2018, p. 36, online: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf> (consulted on March 24, 2020).

prevented diseases in patients[189]. RBT's are technological devices such as: "smartwatches and other wearables, smartphones with health apps, and wireless enabled implanted devices such as pacemakers and blood glucose monitors"[190]. These technologies, as seen previously, use sensors that are able to detect one's state of the body while transmitting and storing the collected data for analysis. Such devices have already been used in clinical trials. For example, in Europe, during a trial, a glucose monitor was used while connected to a smartphone in order to analyze the effectiveness of an artificial pancreas[191]. It was found that this technology does indeed provide better care for patients suffering from certain health conditions such as diabetes or asthma[192].

If we look at the costs of healthcare in Canada, we can see that such technologies could reduce costs while improving people's overall health. As of 2019, healthcare accounts for 11.6% of our GDP, averaging around $ 7,086 per person, with a growth of 4% and is worth $ 264 billion[193]. In 2017, over 60% of the total private and public spending in Canada was a combination of "hospitals (29.5%), pharmaceuticals (16.0%), and physician services (15.3%)"[194]. In these particular areas, RBT's can excel the most while saving costs and increasing the efficiency of healthcare. Moreover, as a population, we will see and feel these changes mainly because this spending comes from our pockets and by saving money in one area, the Government can allocate resources in another one, perhaps more important in the time being. This may also allow the consumer to allocate their money to other things not health related but that will generate revenue for the country. In addition, these gadgets could monitor effectively the use of antibiotic consumption and patients' compliance which could in turn prevent antibiotic resistance, another worldwide problem[195].

---

[189] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 40.
[190] *Id*., p. 61.
[191] *Id*.
Also see: BP KOVATCHEV et al, "Feasibility of outpatient fully integrated closed-loop control", (2013) 36 *Diabetes Care* 1851, on page 1856.
[192] *Id*., p. 62.
[193] CANADIAN INSITUTE FOR HEALTH INFORMATION, *Health spending in Canada reaches $264 billion*, October 31, 2019, online: <https://www.cihi.ca/en/health-spending-in-canada-reaches-264-billion> (accessed on June 20, 2020).
[194] *Id*.
Also see: Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", *Ibid*., p. 63.
[195] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", *Id*., p. 64.
Also see: Ramanan LAXMINARAYAN, et. al., "Antibiotic resistance—the need for global solutions", (2013) 13 *Lancet Infectious Diseases* 1057, on page 1057, online: <https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(13)70318-9/fulltext> (accessed on May 1, 2019).

Moreover, in terms of disease surveillance and its prevention[196], integrating smart health devices into our healthcare system[197], along with what is already done[198], would allow for a more accurate surveillance of upcoming diseases by being able to monitor the point source of an outbreak and monitor its progression before an epidemic can become a pandemic. As with any epidemic, for it to be qualified as such, it would require that incidences increase above an expected number, even if such number is unknown[199]. The expected level of disease is known as the endemic level; it is the observed level. If that level is not high enough to deplete a great number of people, the disease will continue to occur indefinitely. At this point, it becomes important to monitor such diseases to prevent that the endemic level becomes an epidemic. In any case of an outbreak, whether it is common-source, propagated, mixed or other, the number of cases plays a significant role. This means that if such cases can be identified earlier on, it could be possible to stop the spread of an epidemic. Through continuous monitoring, such as it is done with smart health devices, it would be possible to detect outbreaks based on the transmission pattern, identify what type of outbreak that is, where it began and take measures accordingly. The use of this technology, knowing its potential, such as the integration of Google's DeepMind project[200] meant to detect eye conditions, is revolutionary to say the least.

Nonetheless, while most advantages listed above are directly health related, they are not limited to health. Therefore, we would like to showcase some of our findings in a manner that would debunk possible concerns of smart health device users and offer solutions to problematic areas.

---

[196] This is a shared competency between the federal and provincial governments, the latter being responsible for such surveillance and prevention within its province. The federal government would be responsible for this surveillance and prevention when it concerns the entire country or inter-provincial health events. GOVERNMENT OF CANADA, "Canada's Health Care System", online: <https://www.canada.ca/en/health-canada/services/health-care-system/reports-publications/health-care-system/canada.html> (consulted on January 9, 2020).

[197] What we mean by integrating smart health devices into our healthcare system is increasing their usage for health monitoring and using this data to monitor health deviations from users which could lead to an outbreak.

[198] In fact, the Public Health Agency of Canada uses Google Analytics to collect, analyze, measure and report on data about Web traffic and visits. Just as it is done with Google, the Public Health Agency of Canada could partner up with other third parties that own smart health devices to obtain public health surveillance data. GOVERNMENT OF CANADA, "Terms and Conditions", September 19, 2016, online: <https://www.canada.ca/en/public-health/corporate/terms-conditions.html> (accessed on July 24, 2020).

[199] CENTERS FOR DISEASE CONTROL AND PREVENTION, "Principles of Epidemiology in Public Health Practice, Third Edition: An Introduction to Applied Epidemiology and Biostatistics", *Section 11: Epidemic Disease Occurrence*, online: <https://www.cdc.gov/csels/dsepd/ss1978/lesson1/section11.html> (consulted on January 9, 2020).

[200] Katie COLLINS, "Google DeepMind's AI can detect over 50 sight-threatening eye conditions: A focus on artificial intelligence could lead to fewer people losing their sight.", *CNET*, August 13, 2018, online: <https://www.cnet.com/news/google-deepminds-ai-can-now-detect-over-50-sight-threatening-eye-conditions/> (accessed on March 22, 2019); Jeffrey DE FAUW, et. al., "Clinically applicable deep learning for diagnosis and referral in retinal disease", (2018) 24 *Nature Medicine* 1342.

2. The Advantages for the Users of Smart Health Devices

a) Smart Devices Used to Solve Criminal and Civil Charges

Previously, we have examined the risks associated with the use of smart devices and we have determined that a risk associated with their use is the possibility of a breach of one's privacy. Yet, as technology becomes readily available, it does not mean that individuals lose their right to a reasonable expectation of privacy. The definition of what consists of a reasonable expectation of privacy was finally given in 2019 by the Supreme Court in *R. v. Jarvis*.[201] In this case, Mr. Jarvis, a school teacher, used a pen with a camera embedded in it to record students engaging in normal school activities. He was charged with voyeurism under section 162 (1) of the *Criminal Code*. The important take-away from this case is that apart from providing a non-exhaustive list of considerations for this right to privacy[202], the Court noted that individuals still may expect privacy, even in public or semi-public spaces[203], in regards to section 162 (1), but also in everyday life. Indeed, privacy would then not only be expected behind closed doors, but it would depend on the circumstances that one finds themselves in. Additionally, a similar case was previously heard in *R. v. Marakah*[204] where the Supreme Court determined that text messages sent over the phone benefited from this expectation of privacy as "it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging"[205]. The same was concluded in *R. v. Morelli*[206] and futher expanded in *R. v. Cole*[207], but in regards to the information stored on personal computers. It is however important to note that despite having the right to a reasonable expectation of privacy, mobile phones and personal computers[208] are not immune from being searched which could result in the violation of some of our constitutional rights such as sections 7 and 8 of the *Canadian Charter of Rights and Freedom*, essentially violating a person's right to liberty and against unreasonable search and

---

[201] *R.* v. *Jarvis,* 2019 SCC 10 (CanLII).
[202] "[T]hese considerations may include the location where the observation or recording occurred; the nature of the impugned conduct, that is, whether it consisted of observation or recording; the awareness or consent of the person who was observed or recorded; the manner in which the observation or recording was done; the subject matter or content of the observation or recording; any rules, regulations or policies that governed the observation or recording in question; the relationship between the parties; the purpose for which the observation or recording was done; and the personal attributes of the person who was observed or recorded", *R. v. Jarvis*, *Ibid*., par. 5.
[203] *Id*., par. 41.
[204] *R.* v. *Marakah,* [2017] 2 SCR 608, 2017 SCC 59 (CanLII).
[205] *Id*., par.35.
[206] *R.* v. *Morelli,* [2010] 1 SCR 253, 2010 SCC 8 (CanLII).
[207] *R.* v. *Cole,* prev. cited, note 147.
[208] *Laushway* v. *Messervey*, 2014 NSCA 7 (CanLII).

seizure[209]. Seeing both of these smart devices could be searched, thus potentially violating one's right to privacy, the same could be applied to smart health devices which are also not immune to searches and would reveal sensitive information. It is however possible to surpass such violations if the searches are properly documented and serve the purpose related to the arrest[210].

The case *Laushway v. Messervey* is actually quite a novelty in Canada as the Court of Appeal demanded the production of metadata from the plaintiff's computer. This demonstrates that courts are taking interest not only in purely tangible forms of evidence but are also relying on evidence that can be provided by the advancement of technology. This case in particular revolved around a personal injury which demonstrates how "law, technology, and privacy" can come together and sometimes clash[211]. In any case, notwithstanding the technology, the *Laushway* case demonstrates that old legal principles can be applied to new technologies[212]. These ten principles address both reliability and privacy concerns[213]. Yet, with the increase of smart devices and their use, violations of privacy are to be greater than ever. Such metadata gathered by a person's computer can easily be found in RBT's health data; both are also constantly collected, without the user's input being required[214]. The case also mentions the need to develop the jurisprudence in line with our fundamental rights, such as section 8 of the *Canadian Charter*, and to find a balance between seeking justice and ensuring someone's supreme rights. Perhaps the best way to insure this, as mentioned in the case *R*. v. *Vu*, is to seek a warrant before accessing such data[215]. The warrant should also specify the type of data that needs to be collected, the time when the data can be collected, the locations where it can be collected and the depth of access[216]. However, this could violate the privacy rights of people not subject to the warrant because some smart devices act like portals to an area of information shared on networks to which these devices are connected to; hence, people not subject to a warrant could

---

[209] *Charte canadienne des droits et libertés,* prev. cited, note 33, articles 7 and 8.
[210] *R*. v. *Fearon*, [2014] 3 SCR 621, 2014 SCC 77 (CanLII).
[211] Patricia MITCHELL and Jennifer TAYLOR, "Case Commentary on Laushway v Messervey, 2014 NSCA 7; 'Old Evidence Law Dogs, New Technology Tricks", (2015) 12 *Digital Evidence & Elec. Signature L Rev* 13, p. 13.
[212] *Id*., p. 16; *Laushway* v. *Messervey*, prev. cited, note 208, para. 86.
The principles are those of: Connection; Proximity; Discoverability; Reliability; Proportionality; Alternative Measures; Privacy; Balancing; Objectivity; and Limits.
[213] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 79.
[214] *Id*., p. 76.
[215] *Id*., p. 78.
See also: *R*. v. *Vu*, prev. cited, note 137, para. 59.
[216] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", *Ibid*., p. 84.

potentially have their information accessed[217]. Moreover, there should be limits to how the data is treated, meaning only third-party experts should be able to get access and analyze raw data, while extracting only the relevant data which would then be limited by time and location, filtering out private or privileged data[218]. In any case, given the admissibility of the data in Court, it should also demonstrate that it does not meet the test of the "case-by-case privilege" such as it was set out in *Ryan*[219]. It is to note that the psychiatric records in that case did not meet the test's requirements, although they are undeniably private, meaning information gathered from our smart health devices, if used in courts, could have the same outcome. Furthermore, in any decision made by the Court, it must be acknowledged that "public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance the goals of law enforcement"[220]. This is guaranteed by section 8 of the *Canadian Charter*[221].

Moreover, personal health devices could be used to solve murder mysteries which could be beneficial to a collectivity by insuring a safer and healthier environment. Indeed, there are a few examples of such incidences in the United States related to the use of a Fitbit. In one of the cases, Karen NAVARRA, the victim, had deceased following a visit from her stepfather, Anthony AIELLO, who was arrested in 2018 for allegedly taking part of his stepdaughter's murder; this was suggested by the victim's smart health device[222]. Her death was initially framed as a suicide but an autopsy revealed that it was due to trauma. Yet, there were more clues revealing the true nature of her death as her Fitbit showed a spike in her heart rate moments before her death and allegedly during AIELLO's time of visit. In addition, video evidence showed AIELLO's car at the victim's house during the same time frame as when her heart rate spiked and rapidly stopped. The accused deceased from deteriorating health conditions before his trial; yet, were he to live until then, it would have been interesting to see how the devices are used in Court. Furthermore,

---

[217] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 82.
[218] *Id*., p. 81.
[219] *M. (A.)* v. *Ryan*, [1997] 1 SCR 157, 1997 CanLII 403 (SCC), para. 20.
[220] *R*. v. *Vu*, prev. cited, note 137, para. 22.
Also see: *Hunter* v. *Southam Inc*., [1984] 2 S.C.R. 145, 1984 CanLII 33 (SCC), at page 160.
[221] *R*. v. *Vu*, *Ibid*., para. 21.
[222] Louis CASIANO, "California man, 91, linked to stepdaughter's death by Fitbit device dies", *FOX NEWS*, September 12, 2019, online: https://www.foxnews.com/us/91-year-old-linked-to-stepdaughters-death-by-fitbit-device-dies> (consulted on October 24, 2019).
Also see: BBC, "Fitbit data used to charge US man with murder", October 4, 2018, online: <https://www.bbc.com/news/technology-45745366> (consulted on October 24, 2019).

this is similar to a 2015 case involving Richard DABATE, the husband, and Connie DABATE, the wife and victim. Richard blamed the killing of his wife on a home intruder; however, his wife's Fitbit, as stated in an affidavit, discredited his version of events as it computed her movements up to an hour past the alleged time of death given by Richard to the investigators[223].

Additionally, there are not only Fitibt's that can monitor a person's health data, as there were similar cases with Apple Watches. In fact, similarly to the previous cases, the defendant Caroline DELA ROSE NILSSON created a story revolving around her mother-in-law's death but the data gathered on the Apple Watch that Myrna NILSSON was wearing did not coincide with Caroline's story of events[224]. The prosecutor Carmen MATTEO of the Adelaide Magistrates Court stated that "[a] watch of this type … contains sensors capable of tracking the movement and rate of movement of the person wearing it and it keeps a history of the wearer's daily activity, it also measures the heart rate"[225]. Hence, these sensors were used to track the victim's moment of death and demonstrate that at the time the defendant fled from the house to seek help, her mother-in-law had already been deceased for three hours, meaning the defendant potentially had time to stage the scene of the crime. In sum, we have seen that some smart health devices such as Fitbit's and smartwatches can discern time of death amongst many other things.

This type of device could also be interesting in a criminal investigation in order to prove the *actus reus* using data provided by it. The Amazon Echo, for example, was present in a murder scene in November 2015 and was used to solve the murder mystery of a man who drowned in his friend's hot tub[226]. The death was originally blamed on alcohol, however, signs of struggle and data gathered from another smart device, the owner's water heater, revealed an excessive use of

---

[223] BBC, "Fitbit contradicts husband's story of wife's murder – police", April 27, 2017, online: <https://www.bbc.com/news/world-us-canada-39710528> (consulted on October 24, 2019).
See also: Matthew P. KNOX, "Dabate rejects final plea deal", *JOURNALINQUIRER*, January 25, 2019, online: <https://www.journalinquirer.com/crime_and_courts/dabate-rejects-final-plea-deal/article_708b3da6-20c4-11e9-819c-9fc80796d20b.html> (consulted on October 24, 2019).

[224] Rebecca OPIE, "Woman accused of murdering her mother-in-law in Valley View home pleads not guilty", *ABC*, August 23, 2019, online: <https://www.abc.net.au/news/2019-08-23/woman-accused-of-murdering-mother-in-law-pleads-not-guilty/11442382> (consulted on October 24, 2019).

[225] Rebecca OPIE, "Smartwatch data helped police make arrest in Adelaide murder case, court hears", *ABC*, March 29, 2018, online: <https://www.abc.net.au/news/2018-03-29/smart-watch-data-helps-police-find-suspect-in-murder-case-court/9602832> (consulted on October 24, 2019).

[226] Eliott C. MCLAUGHLIN, "Alexa, can you help with this murder case?", *CNN BUISINESS*, December 28, 2016, online: <https://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html> (accessed on March 21, 2019).

water early in the morning. Initially, Amazon refused to give away any information about its users, but later on, when a high-profile attorney took this case and the suspect agreed to his information being handed over, Amazon agreed to provide the data to the prosecutors[227]. Although the information did not incriminate the suspect, it shows that some smart devices are indeed listening to their users; how that information is used and what quantity of it is collected, are other questions that have yet to be answered. Nevertheless, this case further demonstrates that the more smart devices a person owns, the more the information generated on the user increases. In fact, had the suspect been wearing a smart health device monitoring his heart rate, it would have most likely been possible to incriminate him base on a sudden elevated heart rate along with the information retrieved from his other smart devices.

In another case in Ohio, Ross COMPTON was charged with arson and insurance fraud due to evidence that was used against him from his pacemaker and heart monitor[228]. He claimed that a fire had started; however, a low heart rate indicated that there was no hectic escape as he had suggested. If it sounds farfetched and not applicable to those not constantly wearing such devices, many smart devices such as our phone and Fitbit have a built-in step tracker. Such a tool could have been used in order to determine how "active" one was in the event of an Act of God. This, among other things, prevents fraud and illegal activity.

Despite all of the above, such devices can also be used in favor of their user, which was the case in *A1702178 (Re)*[229]. This case pertains to a work-related injury. The worker's job consisted in delivering items to residences. The worker claims that the task had negative effects on her feet, especially after the worker's route had changed, with increased walking adding a strain to her feet[230]. The Workers' Compensation Board that reviewed this case dismissed several times that

---

[227] Eliott C. MCLAUGHLIN, "Suspect OKs Amazon to hand over Echo recordings in murder case", *CNN BUISINESS*, April 26, 2017, online: https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html> (accessed on March 21, 2019).

[228] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 68; Matthew C. CHRISTOFF, "United States: Pacemaker Data May Be Smoking Gun In Aggravated Arson Case", *SEYFARTH SHAW*, February 22, 2017, online: <http://www.mondaq.com/unitedstates/x/570222/Civil+Law/Pacemaker+Data+May+Be+Smoking+Gun+in+Aggravated+Arson+Case> (accessed on March 22, 2019); Cleve R. WOOTSON Jr., "A man detailed his escape from a burning house. His pacemaker told police a different story", *The WASHINGTON POST*, February 8, 2017, online: <https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.d27405b73321> (accessed on March 22, 2019).

[229] *A1702178 (Re)*, 2017 CanLII 95902 (BC WCAT).

[230] *Id.,* para. 11.

her injuries were work related, that is until a letter from her doctor was found, revealing the records of the plaintiff's Fitbit demonstrating that she was walking around 12 km per day[231]. The reliability of the paperwork was contested due to an unusual weekend doctor's appointment. The proof itself was denied by the employer who assured that the new route meant to reduce the walking time and not do the opposite[232]. The worker's union then submitted the data gathered by the worker's Fitbit, being considered the most reliable indicator of the distance walked by the plaintiff[233]. The comparison was made between theoretical data versus raw data; evidently, the latter holds a stronger point. The evidence permitted the Board to conclude that the injury was indeed one developed in the course of employment[234]. The employer's old route required 9.88 km of walking, while the Fitbit calculated 12 km with the new route[235]. The union decided that Fitbit results were more accurate than the theoretical ones produced by a corporate document. The results represented an objective measurement of the length walked by the worker. We should, however, be wary of such decisions because it could open up doors to other wearables being used in courts; such data could be subpoenaed by courts if not willfully provided. This is already the case with some big names including Google, Facebook and Microsoft[236]. Some private companies are even willing to release personal data themselves in order to comply with the law[237].

As we can see, the use of smart technologies by common individuals can be an asset in a law case. However, it could be either a reliable record[238] or be inadmissible in Court due to potential holes in the evidence and the possible willful manipulation of the device and the data provided, while there is always a possibility for the data to be hacked as well[239]. Nonetheless, there is a realistic possibility for such data to be used in Court to favor the user, as seen in *A1702178 (Re)*. It is therefore possible to use the health data provided not to measure a physical injury per se, but

---

[231] *A1702178 (Re)*, prev. cited, note 229, para. 22.
[232] *Id*., para. 24.
[233] *Id*., para. 27.
[234] *Id*., para. 36, 46, 53.
[235] *Id*., para. 45.
[236] Zach MINERS, "Google, Facebook, Microsoft show steady rise in surveillance data requests", *COMPUTERWORLD*, February 3rd, 2014, online: <https://www.computerworld.com/article/2487230/google--facebook--microsoft-show-steady-rise-in-surveillance-data-requests.html> (consulted on February 11, 2020).
[237] Fitbit, "Privacy", online: <https://www.fitbit.com/us/legal/privacy> (consulted on February 11, 2020).
[238] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 67.
[239] Jennifer BROWN, "Data fit for the courtroom?", *CANADIAN LAWYER*, February 2, 2015, online: <https://www.canadianlawyermag.com/author/jennifer-brown/data-fit-for-the-courtroom-2765/> (accessed on March 22, 2019).

to measure the effects of that injury on the plaintiff's activities[240]. This is possible due to the fact that RBT's are able to pick up on "[m]ovement, location, blood pressure, and heart rate"[241] which in their turn compute a user's level of activity. The only physical limitation to this is the desire of the user for his private information to be respected and not be brought to Court, granted it is not subpoenaed or faced with technical limitations making this information inadmissible due to potential tampering of it. In essence, smart health device can benefit the collectivity in numerous ways whether by solving criminal and civil charges or by improving the health of the population. Yet, we can clearly see that, regardless of their use, the development of smart technologies does indeed have a direct impact on user health data.

b) Smart Health Devices Aiding a Population

While smart health devices can be efficient in stopping criminals, they can also serve a greater purpose by aiding those in need. For example, the Apple Watch's movement disorder manager called Movement Disorder API is capable of both measuring and recording progressive symptoms of Parkinson's disease[242]. In fact, smart health devices such as RBT's could detect certain diseases such as Parkinson's disease, hearing problems and other neurological problems[243]. The elderly could certainly benefit from it[244].

The clear benefits of smart health devices turning to healthcare are getting diagnosed before a professional can notice any signs, reducing overall expenditures and time spent at the clinic by increasing diagnoses which can prevent the worsening of health problems requiring long term costs, and being able to track the progression of a health condition at one's fingertips. In January 2018, Apple even announced that its Health App could be connected to hospitals and clinics, therefore giving the users access to their electronic health record (EHR)[245]. Apple has also released Health Records API which gives the developers of third-party apps access to personal

---

[240] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", prev. cited, note 98, p. 67.
[241] *Id*., p. 68.
[242] APPLE DEVELOPER, "Monitoring Movement Disorders", online: <https://developer.apple.com/documentation/coremotion/monitoring_movement_disorders> (consulted on October 25, 2019).
[243] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies […]", *Ibid*., p. 65.
[244] *Id*., p. 72.
[245] APPLE NEWSROOM, "Apple announces effortless solution bringing health records to iPhone", January 24, 2018, online: <https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/> (consulted on October 25, 2019).

EHR[246] to "manage medications, nutrition plans, [diagnose] diseases and more"[247]. On the contrary to a government that has limited financial capacities and needs to allocate its resources not solely in healthcare, it is indeed in Apple's interest to sell such smart health devices. With the popularity of the brand, Apple's watch can reach a great number of people and become a life-saving device. Yet, all smart health devices have their own benefits to individual users and to a population; we shall see how they can be used today in public health monitoring.

In December 2019, we have seen the rise of a new virus called the novel coronavirus dubbed COVID-19 from the Wuhan City in China and it resembles a previous one called Severe Acute Respiratory Syndrome (SARS), but that is deadlier with fatality numbers surpassing the toll of the 2002-2003 SARS outbreak[248]. The World Health Organization has declared that the new coronavirus is a global health emergency as it has killed over 1000 people and had over 43,000 reported cases as of February 11th, 2020[249]. The problem is with the reporting of the cases. The way this virus is transmitted is allegedly from animal to person, then from person to person, and at times the people infected with it may not show any physical symptoms. While the typical symptoms are flu-like such as a fever, coughing and shortness of breath, someone who does not experience the latter may still be infected with the virus and could transmit it to others. Moreover, the incubation period is estimated to be between 10 to 14 days, meaning the virus could be spread without knowing it during that time.

This is where smart health devices should come in. If an infected individual has symptoms and is wearing a Fitbit, their device can measure a sudden change in steps taken in a day and measure an elevated resting heart rate which can signal the presence of a virus before it is known by them or a professional healthcare practitioner[250]. Because of the flu-like symptoms, people may mistake the virus for a common cold or flu without seeing the gravity of their situation and

---

[246] APPLE NEWSROOM, "Apple opens Health Records API to developers", June 4, 2018, online: <https://www.apple.com/newsroom/2018/06/apple-opens-health-records-api-to-developers/> (consulted on October 25, 2019).
[247] *Id*.
[248] ALJAZEERA, "Coronavirus: All you need to know about symptoms and risks", February 11, 2020, online: <https://www.aljazeera.com/news/2020/01/coronavirus-symptoms-vaccines-risks-200122194509687.html> (consulted on February 11, 2020).
[249] *Id*. It is to note that the death toll is increasing daily and has reached six digits as of May 2020.
[250] Andrew BOYD, "Could your Fitbit data be used to deny you health insurance?", *THECONVERSATION*, February 17, 2017, online: <http://theconversation.com/could-your-fitbit-data-be-used-to-deny-you-health-insurance-72565> (consulted on February 11, 2020).

spread it to more people. However, what is known is that the coronavirus has an incubation period of around 14 days and symptoms can start progressively developing in comparison to a common cold or flu that hits you all at once and has an incubation period between 1 to 4 days[251]. Smart health devices can track down the progression of the symptoms and help distinguish between a virus and a common cold or flu. While in both flu and a respiratory virus the heart rate would be elevated, it would technically be possible to distinguish between a virus and flu based on the transmission pattern and incubation period. If two users wear Fitbits for example and user A infects user B, we can calculate how long it takes for user B to get infected. If the incubation period is around one to four days, that could signal the potential presence of the flu[252]. User's B heart rate would then increase within that time frame and the number of steps taken would decrease as well. If the incubation period is around 14 days, this could most likely signal the presence of the new coronavirus. Although such an assessment could be done through human observation, because some people infected with the coronavirus do not experience clear physical symptoms, smart health devices could help detect them before a local epidemic spreads into a pandemic due to diagnosing the correct illness in time. With the help of other more advanced smart health devices, this diagnosis could be made easier and more efficiently.

Indeed, we could potentially be able to distinguish between viruses, as shown by the Stanford Healthcare Innovation lab[253], and be able to track the onset of a virus before it starts spreading to others. In the case of Covid-19, during the 14 day incubation period, the infected individuals might not be aware they have the virus and accidentally spread it to others. Such cases could potentially be identified via sensors that track a user's vitals and stop the spread of the disease by increasing user awareness. Therefore, we also believe that if symptoms of a user are progressively worsening over a period of 14 days, or perhaps still worsening after 4 days, this could suggest the presence of something more serious than the seasonal flu which could require medical attention or immediate isolation. It is indeed possible that different infections could

---

[251] Anna PAUL, "What's the difference between a cold and flu as coronavirus continues to spread?", *METRO*, February 10, 2020, online: <https://metro.co.uk/2020/02/10/whats-the-difference-between-a-cold-and-flu-as-coronavirus-continues-to-spread-12214873/> (consulted on February 11, 2020); Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.

[252] Jill SELADI-SCHULMAN, "Flu Facts: Incubation Period and When It's Contagious", *HEALTHLINE*, October 26, 2018, online: <https://www.healthline.com/health/flu-incubation-period> (consulted on February 11, 2020).

[253] Mike MILIARD, "Scripps, Stanford working with Fitbit to assess wearables' COVID-19 tracking abilities", *HEALTHCAREITNEWS*, April 17, 2020, online: <https://www.healthcareitnews.com/news/scripps-stanford-working-fibit-assess-wearables-covid-19-tracking-abilities> (accessed on Mai 18, 2020).

result in different physiological responses which are shown in varying changes of both heart rate and length of elevation. This was the case with the H3N2 strain that caused a more severe illness than other strains[254]. Hence, differentiation between viruses could potentially be done through the monitoring of varying degrees of illness severity captured by the users' smart health devices. If the differentiation is made possible in the future based on the users' sensory outputs through wearables than it would improve the ability to track diseases and infections and prevent their spread.

The use of these devices can be particularly important in patients with chronic diseases such as diabetes or heart failure and would require real time monitoring[255]. Certainly, the greatest advantage of portable smart health devices is their ability to collect a user's data at any time and any place and transfer it for assessment to healthcare providers[256], doctors, hospitals or even to third-parties that analyze this data and transfer the results directly back to the user for self-management[257]. Moreover, while each individual smart device has its own benefits, the combination of them can prove to be a powerful tool in assessing one's health condition. While smartwatches like the Apple Watch and the Fitbit are on the rise[258], the data generated by them collectively could indicate a health pattern in a community. These devices allow a user to monitor bodily symptoms that were previously solely measured by health practitioners, increase the duration of monitoring and catch issues that might not have been present during a doctor's appointment. Then again, such devices can also help doctors make clearer diagnoses and recommendations based on the data retrieved by the wearables[259]. If this data can be analyzed by

---

[254] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.
[255] Minhee KANG, Eunkyoung PARK, Baek Hwan CHO and Kyu-Sung LEE, "Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices", (2018) 22 *Int Neurourol J*., online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6077937/> (accessed on April 28, 2020).
[256] In fact, smart health devices already allow patients to get a doctor's appointments from the comfort of their home. Simply by having a smart device, they can monitor their health, take pictures of problematic areas and have their devices send the data to their medical professional. This can include the heart rate, blood pressure and any vital signs calculated by smart devices. This does reduce the overall time spent at the doctor's office or in a hospital. CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", prev. cited, note 167, p. 34; it is to note that in Canada "people are not yet in the habit of sharing the health data from their mobile apps with their doctors: only one user out of nine is currently doing this", Guy PARÉ and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 30.
[257] Minhee KANG et. al., "Recent Patient Health Monitoring Platforms […]", *Ibid*.
[258] Chris KRESSER, "The Benefits of Using Wearable Technology for Health Tracking", February 7, 2020, online: <https://chriskresser.com/the-benefits-of-using-wearable-technology-for-health-tracking/> (accessed on April 28, 2020).
[259] *Id*.

health experts, it can also serve public health professionals to make assessments of the health of the general population. Hence, we believe that using smart devices in conjunction with the other data available to public health authorities could potentially save days between the start of an epidemic to the awareness of it. An earlier diagnosis of a disease on an individual level or of an epidemic on a national level can make a difference in the overall death rate. Indeed, as said in a report by the World Health Organization: "to prevent the spread of emerging diseases, it is vitally important to ensure early detection of a new pathogen and the start of human-to-human transmission"[260]. If new ways can be found to detect early health concerns, such as through monitoring the data generated by smart health devices, it could lead to quicker and more effective interventions from national and international entities. Therefore, we cannot help but wonder if the advantages we see on an individual level can be transposed to a nation and even to the world.

Considering all of the above, what needs to be done is to put all this data generated and gathered into action. Such data needs to be accessible to prevent health epidemics on a larger scale. While access to privacy is a key concern of consumers, the true benefits of smart health devices are not individual but collective when different inputs can be compared and analyzed. As a matter of fact, one of the ways this is currently done is through search engines such as Google. When individuals input data online by searching for specific symptoms related to health conditions, this data can be accessed by the Government and can help prevent future health epidemics by analyzing the common trends that are searched within a certain amount of time and at a certain geographic location[261]. Indeed, this type of data gathering has been proven to be successful as shown by an Indian study that demonstrated a strong correlation between some Google search queries in relation to numerous diseases and their outbreaks short after[262]. If the data gathered by smart health devices could be anonymously monitored on a global scale, the benefits would be tremendous. The data would not need to be attached to a particular person, but only extracted from the latter and accessible in a universal database, continuously monitoring the progression of

[260] WORLD HEALTH ORGANIZATION, *Managing epidemics: Key facts about major deadly diseases*, May 2018, pp.19 and 130, online: <https://www.who.int/emergencies/diseases/managing-epidemics-interactive.pdf> (accessed on April 28, 2020).
[261] Madhur VERMA, Kamal KISHORE, Mukesh KUMAR, Aparajita RAVI SONDH, Gaurav AGGARWAL, Soundappan KATHIRVEL, "Google Search Trends Predicting Disease Outbreaks: An Analysis from India", (2018) 24 *Healthc Inform Res* 300.
[262] *Id*.

health conditions worldwide. Once this type of information can be accessed by the World Health Organization, it could increase its efficiency and speed in preventing numerous epidemics which not only impact global health but global economy as well. Essentially, the greatest benefit to sharing personal health information is when such information can stay anonymous while being shared with appropriate authorities capable of analyzing it and implementing effective measure to solve health related issues.

c) Why the Database Solution can Work and Benefit both Users and the General Population

The database solution is feasible as the idea of an IoT-based healthcare system designed to extend healthcare services from hospitals to homes while having the data generated by wireless technology, amongst other resources, assembled in a central server, was already proposed by Yuehong YIN, Yan ZENG, Xing CHEN, and Yuanjie FAN in 2016[263]. Hence, if all healthcare resources of a community can be connected to a central server, so could the data generated by smart health devices and wearables, some of which are already used in healthcare.

Furthermore, just as we predicted above, the use of wearables has already proven to be efficient in tracking diseases such as the seasonal flu[264]. As a matter of fact, the employment of secondary signals coming from "heart rates, physical activity and sleep quality", which are found in Fitbit trackers, amongst other devices, could predict the spread of the flu even better than through current disease surveillance methods and can do so in real time[265]. Indeed, as suspected previously, our bodies react differently based on our health condition and our vitals tend to be abnormal. In the case of a seasonal flu or of an acute infection, our resting heart rate will be elevated, usually accompanied by a fever suggesting the body is fighting off an infection, and an infected person will tend to change their daily routine due to changes in their body such as sleep and activity patterns[266]. The sleep is more likely to increase whereas the daily activities are likely

---

[263] Yuehong YIN, Yan ZENG, Xing CHEN, and Yuanjie FAN, "The internet of things in healthcare: An overview", prev. cited, note 76, point 2.2. They believe that "an IoT-based system makes it possible to provide 'one stop' service to the residents conveniently even at remote locations [and] [it] may be […] used world widely".

[264] Conor HALE, "Fitbit for the flu: Researchers show the fitness wearables can help track outbreaks", *FIERCEBIOTECH*, January 17, 2020, online: <https://www.fiercebiotech.com/medtech/fitbit-for-flu-researchers-show-fitness-wearables-can-help-track-outbreaks> (accessed on May 1, 2020).

[265] *Id*.

[266] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, "Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study", prev. cited, note 179.

to decrease. To test the correlation between the use of wearables and the prediction of diseases such as the influenza flu, The Lancet Digital Health examined 47 249 regular users of the Fitbit in the top five U.S. States with the most Fitbit users[267] by using de-identified data[268] generated by their wearables and evaluated over 13 million resting heart rate and sleep measures[269]. The results were used to track any deviation from personal norms. In fact, tracking physiological changes over time in comparison to personal norms can successfully identify irregularities in a person's health. All abnormal readings were then compared to weekly estimates of the rate of people with flu-like symptoms. What was discovered is that "[w]]eek-to-week changes in the proportion of Fitbit users with abnormal data were associated with week-to-week changes in ILI rates in most cases"[270]. Hence, using the data generated by Fitbits improved the predictions of flu-like diseases in the five States studied during the experiment. The interpretation given in this study supports the solution given in this thesis. Indeed, smart health devices and wearables have activity and physiological trackers which are used more and more in the United States but also throughout the world to monitor one's health. The data generated by them reveals real-time data and the location of the devices which enhances geographical surveillance of diseases. As said by Jennifer M. RADIN et. al., the information retrieved by these devices can be of high importance when it comes to enacting outbreak response measures in a timely manner in order to either prevent the transmissions of diseases during an outbreak or to diminish the spread of it[271].

The reason why wearables are a great addition to disease monitoring is because the current methods of monitoring flu-like illnesses may take from one to three weeks while wearables reveal real-time data. In fact, other monitoring techniques have been tested, as discussed above, such as Google Flu Trends, but the problem with the latter is that it overestimated the number of people infected during the 2009 H1N1 pandemic[272]. Surveillance through social media such as Twitter was also tested but the results were mixed in terms of the success of depicting an accurate representation of infected people. The biggest problem with these rapid techniques of crowd-sourced data, known as nowcasting, is personal identification and relating the data to a

[267] The five states were: California, Texas, New York, Illinois, and Pennsylvania.
[268] This process and term is similar to the one proposed in this thesis which consists in keeping the data anonymous by preventing PII from being revealed to ensure users' privacy.
[269] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.
[270] *Id*.
[271] *Id*.
[272] *Id*.

user, for example, rather than to someone else. What we mean by this is that in contrast to social media and the Internet where search queries might not relate to one's own state of being, wearables are connected to a user and generate data based on a user's own input. A user's symptoms cannot relate to someone else's but search queries can be of simple curiosity or be done for someone else which can heighten overall statistics, especially on a State level[273]. Additionally, wearables provide objective data and have "significantly improved nowcasting of influenza-like illness"[274]. While crowd-sourced data is affected by outside factors, sensor-based data offers real-time measurements of a disease in a given population. Nevertheless, more studies would be required to distinguish between what are considered to be deviations from normal levels caused by infectious in contrast to non-infectious diseases. In any case, we can confidently conclude that wearables can indeed track and monitor diseases, whether they are severe or not. The benefits are numerous and more so if the data gathered comes from different regions of the world, especially in areas where surveillance of diseases is not possible. The greater the volume of data to analyze, the more geographically refined the surveillance through sensors can be. Such monitoring on a national level would improve the efficiency and precision of public health responses, while the same impact could potentially be seen internationally by the World Health Organization. While the study discussed above only used a Fitbit tracker and concluded on its efficiency in disease monitoring, we believe that having the data of multiple different wearables can increase precision and accuracy through the many sensors available.

Currently, the Public Health Agency of Canada is using its FluWatchers program to monitor the evolution of the Coronavirus[275]. The program is usually meant to track the spread of the flu and flu-like-symptoms. Nevertheless, it works by sending recipients two questions weekly to determine if they had a cough or a fever the previous week. This data helps track the location of COVID-19. The higher the number of participants, the more accurate the information will be. As we can notice, this is similar to the idea we propose but less accurate. If the participants of the FluWatchers program would agree to share their personal health data from their wearables which

---

[273] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.
[274] *Id*.
[275] Jean-Benoit LEGAULT, "FluWatchers pour surveiller la COVID-19", *LA PRESSE*, April 5, 2020, online: <https://www.lapresse.ca/covid-19/202004/05/01-5268086-fluwatchers-pour-surveiller-la-covid-19.php?fbclid=IwAR2AhGoJGT9MeiYZ6PC3BqlKPu78v4Brb9OQKDNyXZNrxsuzRKgi2VYQIt4> (accessed on May 7, 2020).

can be retrieved and analyzed by the Public Health Agency of Canada in a national database, then we could increase the accuracy of the data and determine more easily which areas are the most affected by the virus. As it is possible to notice, the FluWatchers program is meant to track the spread of the flu and flu-like-symptoms, but as seen, wearables such as the Fitbit are capable of doing the same, and they do so continuously, on a daily basis. Additionally, instead of questions that could be answered with a bias, the wearables would provide objective data capable of enhancing the current method of disease surveillance.

Another example of a smart health device tracking the spread of a virus is the Kinsa smart thermometers. These thermometers connect to a mobile application via Bluetooth and reveal the users temperature along with signs of fever and illness. The information collected is aggregated into anonymized datasets which can be geographically separated. These thermometers have been able to track the spread of COVID-19 in nearly real time. They also found a way to differentiate between the flu and the coronavirus: "Sudden spikes in fevers detected by the thermometers, beyond what one expects from typical flu numbers, may reveal coronavirus cases instead"[276]. As well, as the geographical location is computed, spikes in certain regions can help locate outbreaks and follow their transmission pattern.

In any case, both the influenza and COVID-19 are contagious and can be deadly. While differentiating between them will take further studies, knowing when to self-quarantine or to take precautions can reduce the risks of increasing the spread of the disease. Moreover, while it may be hard to take appropriate measures on an individual level when a serious illness arises, the Government can use de-identified data to take the necessary precautions in time. Once public health authorities get a hold of this data, they can evaluate if incidences increase above an expected number, above the endemic level. If they see a sudden rise in behavioral and physiological changes, they can take appropriate measures early-on. If Fitbits have improved the predictions on a State level[277], so can other smart health devices whose data is generated and stored in a national database. Having an early detection mechanism of viruses is an important

[276] Charlie OSBORNE, "From flu to coronavirus: Smart thermometers deployed to track the spread in real-time", *ZDNET*, March 19, 2020, online: <https://www.zdnet.com/article/smart-thermometers-deployed-to-track-coronavirus-spread-in-real-time/> (accessed on May 8, 2020); Donald G. MCNEIL Jr., "Can Smart Thermometers Track the Spread of the Coronavirus?", *THE NEW YORK TIMES*, March 18, 2020, online: <https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html> (accessed on May 8, 2020).
[277] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.

part in taking appropriate measures such as pharmaceutical[278] and non-pharmaceutical interventions meant to prevent the future spread of the virus and its infection of the population[279]. More so, multimodal assessment through the use of different wearables with "sensors for temperature, blood pressure, pulse oximetry, ECG, or even cough recognition"[280] would further improve the detection and differentiation of arising diseases. Moreover, with continuous improvement in viral disease detections, it could be possible to identify influenza-like illness rates daily and these surveillance techniques could be applied on a global scale.

In addition, surveillance through smart health devices such as it is done through Internet-based surveillance[281] could prove to be very efficient, especially for the WHO. In fact, during the Severe Acute Respiratory Syndrome (SARS) outbreak in 2002 and 2003, which was similar to the new coronavirus, The Global Public Health Intelligence Network (GPHIN) successfully detected an outbreak in China through event-based surveillance from varying online sources such as websites and electronic forums, and alerted the WHO just in time to implement an international response[282]. In countries with weak or almost nonexistent public health surveillance, this could provide real-time data on disease activity by country or by region. At the moment, the GPHIN receives information from the Internet and news coverage of health events and uses this information to detect early signs of an outbreak[283]. A monitoring system similar to the GPHIN could be implemented by additionally analyzing personal health data. While other monitoring techniques already exist, such as through the increase in the purchase of certain medication[284] and through web-based tools such as Google Flu Trends that analyze web queries[285], the problem with such surveillance methods is that they require a high number of

[278] These would include developing and deploying antivirals and vaccines earlier on.
[279] These could include a quarantine, self isolation, or increasing the amount of times we wash our hands.
[280] Jennifer M. RADIN, Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, prev. cited, note 179.
[281] Eirini CHRISTAKI, "New technologies in predicting, preventing and controlling emerging infectious diseases", (2015) 6 *Virulence* 558, on page 559.
[282] *Id*.
[283] Eric MYKHALOVSKIY and Lorna WEIR, "The Global Public Health Intelligence Network and early warning outbreak detection: a Canadian contribution to global public health", (2006) 97 *Can J Public Health* 42-4, online: <https://www.ncbi.nlm.nih.gov/pubmed/16512327>.
[284] Eirini CHRISTAKI, "New technologies in predicting, preventing and controlling, *Ibid*., p. 559.
[285] *Id*., p. 560. This works by monitoring the number of people that search different keywords; this number correlates to the amount of people that have a certain health issue. To note that Google Flu trends was shut down by Google in 2015 because it was criticized for overestimating the flu prevalence. Their technology was handed over to nonprofit organizations like HealthMap which use Google data and build their own outbreak maps: <https://healthmap.org/en/>; Matt O"BRIEN and Christina LARSON, "Can AI flag disease outbreaks faster than humans? Not quite", prev. cited, note 17.

users to be effective, especially in developed countries. Hence, monitoring the progression of different diseases through smart health devices would increase the level of accuracy even with a limited quantity of users. This is because such devices have numerous sensors and are capable of monitoring, storing and analyzing most health-related information. As well, the geolocation feature on some of the smart devices could pinpoint the exact location of an outbreak, leading to effective measures taken by appropriate authorities, namely quarantines, if need be. Precisely, a study has shown that mobile phones can track the users' movements and identify the routes of importation of infectious diseases while following its transmission pattern[286]. Withal, with the growth in network coverage, this type of monitoring can even be done in countries that have limited resources such as it has been done in Sri Lanka to monitor animal health[287].

While considering the database solution, a problem to lookout for is the access of one State to personal health statistics of another State. A negative evaluation could impact the economy of the affected country by becoming isolated by the rest of the world which is known as the "prisoner's dilemma"[288]. Another problem is with temporal asymmetry as other countries can quickly impose trade sanctions against the affected countries but they are not so quick to lift them once the health crisis has been averted or solved[289]. Countries constantly seek to balance their power and if it is not done with weapons or wealth, it could be done through research and sanctions. This is why it is important to find a solution both globally accepted and individually by the primary producers of such data, without compromising their right to privacy in the process; a right recognized by the Supreme Court of Canada in *R*. v. *Dyment*[290].

---

[286]Eric MYKHALOVSKIY and Lorna WEIR, "The Global Public Health Intelligence Network and Early Warning Outbreak Detection: A Canadian Contribution to Global Public Health", (2016) 97 *Canadian Journal of Public Health* 42, p. 563.

[287] Jo HALLIDAY, et. al., "Bringing together emerging and endemic zoonoses surveillance: shared challenges and a common solution", (2012) 367 *Philos Trans R Soc Lond B Biol Sci*. 2872.

[288] Johan GIESECKE, "8. International Health Regulations and Epidemic Control", *WORLD HEALTH ORGANIZATION*, online: <https://www.who.int/trade/distance_learning/gpgh/gpgh8/en/index2.html> (accessed on October 25, 2019).

[289] The WHO tries to mitigate some of these risks as seen in the International health regulations of 2005 which seeks "to prevent, protect against, control and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks, and which avoid unnecessary interference with international traffic and trade", *International Health Regulations (2005)*, May 23, 2005, (2007) 2509 R.T.N.U. 79 (n° 44861), online: <https://apps.who.int/iris/bitstream/handle/10665/246107/9789241580496-eng.pdf;jsessionid=308F5DBEB01C81824C21D940B0256EC0?sequence=1> (accessed on July 25, 2020).

[290] "[…] society has come to realize that privacy is at the heart of liberty in a modern state […]. Grounded in a man's physical and moral autonomy, privacy is essential for the well- being of the individual […]". *R*. v. *Dyment*, [1988] 2 S.C.R. 417, par. 17; Philippe BRAILLARD, *Théories des relations internationales*, prev. cited, note 25.

In essence, we have seen some of the risks users of smart devices might encounter. These risks reappear in smart health devices but can be increased due to the sensitive nature of the information retrieved from smart health devices. Users are then faced with a potential violation of their right to privacy which increases the more they use their device and the more of them they use. The Government also faces risks in enacting our proposed solution as health data is not only sensitive but it is also lucrative on the black market. Nonetheless, while privacy concerns are on the rise with the use of these devices, so are the benefits. We have briefly seen that individuals may greatly benefit from these devices to monitor their health, while the Government can also benefit from the information generated to better monitor public health concerns. Nonetheless, the true advantage derives from improving the health of a nation by monitoring flu-like symptoms in a population and preventing the rise and the spread of diseases. However, in order for the benefits to outweigh the consequences, it is crucial to mitigate potential risks before enacting the proposed solution. This way it would be possible to reduce privacy violations while enhancing the health of a population. The improvement of healthcare should not infringe on our rights.

II. Making the Most out of Smart Health Devices: A National and International Database

Individuals should not have to choose between health and their fundamental rights. While this thesis attempts to determine if the aforementioned risks can be acceptable in exchange of better health assessments and an overall increase in collective health and wellbeing, we believe that individual privacy can be maintained and the healthcare system improved if we take the appropriate course of action to mitigate potential risks and to favor the advantages. Indeed, there are a few things that both the Government and the users of smart devices can do to mitigate the risks or to counter them such as through legal available remedies. While it may not always be possible to prevent all risks associated with the use of smart health devices, it should be possible to mitigate the risks whether it is achieved in a preventative way or in response to a violation of one's rights. Once the risks are mitigated, both users and the Governments can favor their

---

Moreover, it is important to tackle user concerns regarding the right to privacy before enacting the proposed solution. Concerns such as "that unauthorized third parties will make inappropriate use of personal data" or "with the possibility of intrusion into individual privacy", especially considering that the "use of mobile health apps [and smart health devices], is a relatively recent phenomenon in Canada, but we should expect that this use will spread quickly" Guy PARÉ et. al., *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 51 and 25.

advantages such as through the creation of a national and international database to enhance the benefits generated by the use of smart health devices. Therefore, we shall list a few ways smart device users and the Government can mitigate some of the risks before demonstrating how they can favor their advantages through the use of smart health devices in public health monitoring.

A. How to Mitigate the Risks of Smart Health Devices

1. Smart Device Users

As we demonstrated earlier in the thesis, the risks of using smart health devices are numerous in terms of privacy. While some of these risks derive from third parties or unauthorized persons getting access to user data, other risks arise straight from the source, from the use of such devices and their initial collection of data on users. Indeed, the fact that these devices collect a high amount of sensitive data on its users and that such data can be aggregated to other information generated by smart devices connected to the Internet of Things makes users more vulnerable to privacy breaches. However, it is possible to mitigate or to counter such risks in a way that users of smart health devices benefit from their gadgets with less fear surrounding their right to privacy. While there will always be risks associated with the use of smart health devices in regards to the protection of our personal information, many things can be done on the individual level to minimize the risks associated with our rights and our information accessed, to insure that our own devices and laws are not used again us nor betray our confidence.

a) Mitigating Legal Risks

Discrimination:

In order to improve overall global health, trade-offs have to be made, and it is our personal health data that would be directly affected, or more precisely our right to privacy. Indeed, our personal medical records could potentially be accessed by employers and health insurance companies. Although both require the client's consent due to the laws we have previously covered, it may be impossible for the latter to get the desired job or a health insurance if such information is not provided. This would technically be illegal in Quebec[291] under the

[291] See section 18.1 of the *Charter of human rights and freedoms*, prev. cited, note 105.

Quebec Charter, although companies do find workarounds. This could lead to discrimination based on health, under the ground of physical disability of section 15 (1) of the *Canadian Charter* if such discrimination were to be inflicted by the Government; similarly, this could lead to discrimination under section 10 of the *Charter of human rights and freedoms*[292] under the ground of handicap. The latter could apply both to the public and the private sector. As a matter of fact, obesity or an elevated body mass index (BMI)[293] is considered a handicap and any inequitable treatment for weight conditions could be considered as discrimination[294].

Indeed, we may be quick to jump on newly available gadgets and opportunities when they seem to benefit us, but by doing so, we naively miscalculate the costs. Say we take the John Hancock's Vitality program[295] in the United States for example; it offers a rebate of 15% off its life insurance to customers who agree to share data regarding their health by wearing a free Fitbit. Users of this program get points for staying healthy and active, for not consuming tobacco and for getting annual health screenings[296]. This is also offered in Canada, operating as Manulife instead of John Hancock. Manulife offers a smartwatch at a discounted price and a potential reduction of life insurance fees in exchange of the information gathered by the device[297]. How it works: the more you are active, the less you pay. Perhaps while saving on monetary costs, the user pays in data costs.

As mentioned by Pierre TRUDEL, such devices are able to pinpoint user's behavior impacting their health and insurance companies could use this knowledge and refuse to insure someone on

---

Also see: ÉDUCALOI, "The Right to Access Medical Records", online: <https://educaloi.qc.ca/en/capsules/the-right-to-access-medical-records/> (accessed on July 25, 2020).

[292] *Charte des droits et libertés de la personne*, prev. cited, note 105.

[293] CENTER FOR DISEASE CONTROL AND PREVENTION, "Defining Adult Overweight and Obesity", June 30, 2020, online: <https://www.cdc.gov/obesity/adult/defining.html> (accessed on July 25, 2020).

[294] Harriet NOWELL-SMITH and Hugh O'REILLY, "A Triumph of Substance Over Form in How Discrimination Law Treats Obesity", (2003) 82-3 *Canadian Bar Review* 681, online: <http://www.canlii.org/t/2cjq> (consulted on October 28, 2019);

Also see : Malgorzata ULLA, "L'obésité d'un travailleur constitutive d'un handicap relevant de la protection de la Directive 2000/78 – L'évolution récente de la notion de handicap en droit de l'Union européenne", (2015) 28-1 *Revue québécoise de droit international* 185, online : <http://www.canlii.org/t/2sbv> (accessed on October 8, 2019).

[295] JOHN HANCOCK, "John Hancock Vitality", online: <https://www.johnhancockinsurance.com/vitality-program.html> (accessed on March 21, 2019).

[296] Matt HAMBLEN, "As smartwatches gain traction, personal data privacy worries mount", *COMPUTERWORLD*, May 22, 2015, online: <https://www.computerworld.com/article/2925311/as-smartwatches-gain-traction-personal-data-privacy-worries-mount.html> (accessed on March 21, 2019).

[297] MANULIFE, "Get your Apple Watch", online: <https://www.manulife.ca/personal/vitality/vitality-for-individuals/apple-watch.html> (accessed on March 27, 2019).

this basis[298]. Another problem with such devices is that, despite their accuracy, they can produce false-positives. Hence, on one side, such sharing of information provides additional benefits for the users, but on the other side, fallen into the wrong hands, accessing someone's poor results can be detrimental to their career, especially if health is a big factor. Nonetheless, we could question if such risks are worth taking considering that the data assembled could predict and prevent heart disease or diabetes in the future. Yet again, if such information were to come into the hands of potential employers, it could lead to new types of discrimination not accounted for by the private sector legislation such as the *Quebec Charter*. While there are resources and legal remedies against discrimination as defined in both Charters[299] and in the *Canadian Human Rights Act*[300], all other forms of unequal treatment that do not fall under a reason of discrimination could persist. As a matter of fact, laws protecting citizens from discrimination in the private sector are exhaustive and they do not account for other forms of discrimination such as it is done in the *Canadian Charter*. Furthermore, health is not accounted for as a ground for discrimination in the *Quebec Charter* unless it is linked to another ground such as a handicap. While there are means to attach a certain health condition to a handicap, such as obesity, what this means for the private sector and users of smart health devices is that their personal sensitive information could potentially be used to legally "discriminate" against them based on their overall health without it being considered as discrimination.

Yet, we ought to remain hopeful that if a situation of injustice occurs, that laws will protect us from it. As a matter of fact, we have already been seeing a genetic discrimination in this country[301]. The *Genetic Non-Discrimination Act* had been adopted in 2017 to cover such matter[302], although the constitutional validity of the law had been questioned recently. Nonetheless, it would be a matter of time before new forms of "discrimination" appear or

---

[298] Annie DESROCHERS, "Quand des médecins recommandent de porter une montre intelligente", *ICI RADIO-CANADA*, February 21, 2019, online : <https://ici.radio-canada.ca/premiere/emissions/le-15-18/episodes/427492/audio-fil-du-jeudi-21-fevrier-2019/16> (accessed on March 27, 2019).

[299] *Charte canadienne des droits et libertés*, prev. cited, note 33.
See also : *Charte des droits et libertés de la personne*, prev. cited, note 105.

[300] *Canadian Human Rights Act*, R.S.C. 1985, c. H-6.

[301] Yann JOLY and Gratien DALPÉ, "Vers une discrimination génétique au Canada?", *DROIT INC.*, March 19, 2019, online : <http://www.droit-inc.com/article24362-Vers-une-discrimination-genetique-au-Canada?fbclid=IwAR0D-8DEuLHcGAbD0rdIVKUyu16Nevnzt8wzG4wL3GLiw5qDE-ZskdFWsWA> (accessed on March 21, 2019).

[302] *Genetic Non-Discrimination Act*, S.C. 2017, c. 3; *In the matter of the: Reference of the Government of Quebec concerning the constitutionality of the Genetic Non-Discrimination Act enacted by Sections 1 to 7 of the Act to prohibit and prevent genetic discrimination*, 2018 QCCA 2193 (CanLII).

"unequal access to work opportunities"[303]. Considering the possibility that employers get access to personal data such as the number of times an employee has gone to use the bathroom, has taken breaks, or worse, has developed health issues, it could inevitably lead to a violation of their fundamental right to privacy. Even so, some authors have shown that "employees who disclose their mental health conditions may face restricted opportunities, micro-management, subtle forms of social exclusion (including being the subject of gossip) and the possibility of having mistakes over-attributed to their illnesses"[304]. It is also said that "[o]ne in five employees living with a serious mental illness report experiencing job-related discrimination such as being refused a transfer, having difficulty accessing training and professional development and not advancing on the job through promotion"[305]. What if their choice gets taken away from them? These are some risks employees might inevitably face. Yet, while such disclosure would violate their right to privacy, they could benefit from work related accommodations as provincial and federal legislation obliges employers to accommodate their employees, if it is a reasonable accommodation and does not cause undue hardship[306]. A further problem may however arise from the possibility to legally justify discrimination. There are a few possibilities to do so such as through section 1 of the *Canadian Charter*; section 9.1 for articles 1-9 and sections 20-20.1 for article 10 in the *Canadian Human Rights Act*; and section 15 in the *Quebec Charter*. Yet, in any case, the employer must "take all reasonable measures to accommodate, short of undue hardship, in order to avoid discrimination"[307]. Additionally, courts would accept discrimination if the bona fide occupational requirement (BFOR) as developed in *British Columbia (Public Service Employee Relations Commission)* v. *British Columbia Government and Service Employees' Union (B.C.G.S.E.U.)*[308] is fulfilled and justified.

---

[303] Nicholas CAIVANO, "Inaccessible Inclusion: Privacy, Disclosure and Accommodation of Mental Illness in the Workplace", (2016) 5-1 *Canadian Journal of Human Rights* 97, 2016 CanLIIDocs 69, on page 99 <http://www.canlii.org/t/6x1> (retrieved on 2020-03-23).

[304] *Id*., p. 99; Patrick CORRIGAN & Robert LUNDIN, *Don't Call Me Nuts: Coping with the Stigma of Mental Illness*, Illinois, Recovery Press, 2001.

[305] Marjorie L. BALDWIN & Steven C MARCUS, "Perceived and Measured Stigma Among Workers with Serious Mental Illness", (2006) 75:*3 Psychiatric Services* 388.

[306] Nicholas CAIVANO, "Inaccessible Inclusion: Privacy, Disclosure and Accommodation of Mental Illness in the Workplace", *Ibid*., p. 101; Laura BARNETT, Julia NICOL & Julian WALKER, "Background Paper: An Examination of the Duty to Accommodate in the Canadian Human Rights Context", (2012*) Library of Parliament* at 2, online: <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201201E>.

[307] Laura BARNETT et. al., "Background Paper: An Examination of the Duty to Accommodate […]", *Ibid*., at 2.3.

[308] "A three-step test should be adopted for determining whether an employer has established, on a balance of probabilities, that a prima facie discriminatory standard is a bona fide occupational requirement (BFOR). First, the

Moreover, while the scenario of an employer getting access to an employee's personal health data through their smart health devices is hypothetical, if such a violation does occur, there will be legal remedies available such as section 3 of the *Civil Code of Quebec* which protects the right to privacy. In addition, section 1457 of the *Civil Code of Quebec* could then be used to prove the social ramifications related to the exposure of personal health information, such as damage to their career, dignity and reputation. In any case, the way to mitigate or to counter risks is through the legal remedies available. Users of smart health devices can therefore be assured that if their personal health data is accessed without consent and used to discriminate them, the legislation in place will be there to protect them. Nonetheless, to mitigate such risks along with the risk of facing a potentially legal discrimination, users of such devices should seek out the motive for their refusal, whether for a job or an insurance, to make sure that employers or insurance companies are not illegally using their PHI against them. It is part of individual due diligence to protect ones personal data from the grasp of those who seek to obtain it, through legal or illegal means. Furthermore, if health data is a work or an insurance necessity, Section *c) Mitigating our own Actions*, will demonstrate what individuals may do to reduce the amount of data computed on them through their wearables and smart devices to avoid privacy violations.

Unreasonable Search or Seizure:

Nonetheless, a bigger legal problem arises when the seizure of such devices violates section 8 of the *Canadian Charter of Rights and Freedom* which states that "[e]veryone has the right to be secure against unreasonable search or seizure"[309]. Although this text is

---

employer must show that it adopted the standard for a purpose rationally connected to the performance of the job. The focus at the first step is not on the validity of the particular standard, but rather on the validity of its more general purpose. Second, the employer must establish that it adopted the particular standard in an honest and good faith belief that it was necessary to the fulfilment of that legitimate work-related purpose. Third, the employer must establish that the standard is reasonably necessary to the accomplishment of that legitimate work-related purpose. To show that the standard is reasonably necessary, it must be demonstrated that it is impossible to accommodate individual employees sharing the characteristics of the claimant without imposing undue hardship upon the employer", *British Columbia (Public Service Employee Relations Commission)* v. *British Columbia Government and Service Employees' Union (B.C.G.S.E.U.)*, 1999 CanLII 652 (SCC), [1999] 3 S.C.R. 3.

[309] *Charte canadienne des droits et libertés*, prev. cited, note 33.

The law should be able to adapt accordingly. Having the categories mentioned by Lee-Ann CONROD would seem to be a more efficient solution than the one proposed by Justice BINNIE in *R*. v. *Tessling*, which suggests using a case by case approach based on the evolution of technology which causes uncertainty in the law, *R*. v. *Tessling*, [2004] 3 SCR 432, 2004 SCC 67 (CanLII), para. 29. These categories do indeed provide some predictability. In fact, Justice BINNIE had to determine in *R*. v. *Tessling* whether or not a search using FLIR technology intruded on the defendant's reasonable expectation of privacy. However, instead of classifying this type of technology into a group,

straightforward, it is not the case with the jurisprudence as some defendants have argued before the Supreme Court of Canada that their right to privacy has been violated following the seizure of smart devices that were used against them[310]. A greater legal certainty should therefore be established through laws or uniform jurisprudence.

The problem with section 8 arises when the State intrudes on individual's privacy. Yet, at what point do we define what constitutes legal or unlawful searches of smart devices in regards to section 8? Moreover, is the seizure of personal health information ethical? The answers to these questions could help us determine whether the limitation of our right to privacy is justified for the purpose of improving global health.

The matter of the fact is, as we connect to the Internet of Things through wearable technology or connected automation systems such as smart light bulbs, we unconsciously exchange our privacy for the perceived benefits we get from such systems handling our personal information and making our lives easier. This exchange comes at a price as making our lives easier costs us the recording, collecting, transmitting, storing and analyzing of our data along with giving away details about our whereabouts such as our exact location, our finances and even gives access to our sensitive information, namely health data[311]. At the end of the day, we make a choice and our choices generate consequences. For example, if a person chooses to break the law, they also make the choice of potentially facing a legal consequence, and at times, underestimate the risks of getting caught. Such is the case with smart devices. If a user makes a choice to use them in order to make their life easier, then they also make the choice of sharing their personal data with the developers and even perhaps different third parties; this being said, their decision might not be a conscious choice as they too can underestimate the risks. The ethical question becomes tricky when a person does not have a choice and does not consent to the disclosure of their

---

Justice BINNIE decided it is better to "deal with […] privacy implications at that time in light of the facts as they then exist", *R*. v. *Tessling*, *Id*., para. 29. Indeed, while looking at current technological capabilities and not their potential capabilities would seem to be the right way to go, leaving it as such causes uncertainty which can be removed with the above mentioned categories. Without this certainty, violations of section 8 of the Canadian Charter are more likely to happen. Yet, even if such violations are noticed by the Court, the evidence might still be admissible due to the uncertainty in the law, Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7, p. 124. Hence, knowing the different types of technology and their levels of privacy protection can help reduce both uncertainty and violations of our fundamental rights.

[310] Lee-Ann CONROD, "Smart Devices in Criminal Investigations […]", *Ibid*., p. 116.

[311] *Id*., p. 116.

information. A person may find themselves facing a moral dilemma that can transcend into a legal one. Indeed, users of smart health devices have a choice: to use such devices and potentially have their right to privacy violated, or to seek an alternative by abstaining from using them and risk their health or even their lives[312]. As one might notice, the choice here is a mere illusion because the true choice is between a hospital bed and being free physically, but not from the grasp of those who seek to benefit from personal data. Therefore, we can say that the choice is between giving up one's freedom or to be scrutinized by the legal system[313]. The only reasonable way we see fit to violate one's privacy is when the violation can benefit a society by outweighing individual consequences, and can be justified in a free and democratic society, such as it is stated in section 1 of the *Canadian Charter*. We believe that using the data provided by smart health devices to provide feedback to those who cannot often visit a medical professional is one example of a morally and legally acceptable way of using someone else's information; it is more so when the latter is used to improve global health and provide quicker remedies to epidemics. Therefore, having established the moral basis of sharing personal health data, the legal uncertainty regarding section 8 of the *Charter* needs to be addressed.

Section 8 of the *Canadian Charter of Rights and Freedoms* states that "[e]veryone has the right to be secure against unreasonable search or seizure"[314]; it requires a flexible interpretation to be able to adapt to changes over time along with societal values. Indeed, this was the interpretation given by Justice DICKSON in *Hunter* v. *Southam*[315]. Nonetheless, this section is limited to State intrusion on individual privacy and does not apply to private parties. It is however possible to challenge a State intrusion through section 24 (2) of the Charter in order to exclude evidence from Court. It is also to note that while section 8 protects against unreasonable search and seizure, it allows solely a reasonable expectation of privacy[316]. This was reiterated in the decision *R* v. *Cole* mentioned previously[317]. Nevertheless, while it was noted in this decision that using a work computer instead of a personal computer lowered the expectation of privacy of the accused,

---

[312] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies in Healthcare and the Law", prev. cited, note 98, pp. 70-71; K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 25.
[313] *Id*., p. 71.
[314] *Loi constitutionnelle de 1982*, annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.), PART VII.
[315] *Hunter et al.* v. *Southam Inc.,* [1984] 2 SCR 145, 1984 CanLII 33 (SCC), p. 152.
[316] *Id*., p. 159.
[317] *R. v. Cole*, prev. cited, note 147, para 35.

in comparison to using a personal computer, the Supreme Court granted the accused a reasonable expectation of privacy. As such, the question is much simpler when there is no reasonable expectation of privacy because section 8 would not apply, whereas when there is a reasonable expectation of privacy, a second question must be answered which is if the search or seizure was unreasonable and intruded on one's privacy[318]. Therefore, a search conducted following a warrant is presumed reasonable even if it invades a person's expectation of privacy[319]. However, there is also a possibility to apply for prospective warrants. As seen in *R.* v. *Vu*, Justice CROMWELL has explained that the "police may discover computers in a range of situations and it will not always be appropriate to require specific, prior judicial authorization before they can search those devices"[320]. This means that law enforcement authorities might not always need authorization before searching electronic health devices, allowing for a void and uncertainty of the law in place. Therefore, even if a Court finds a breach of section 8 of the *Canadian Charter*, it might allow the evidence due to said uncertainty in the law. In addition, Justice BINNIE clearly noted in *R.* v. *A.M.* that when analyzing the violation of section 8, it is important to take into account three considerations which are: "minimal intrusion, [specific] nature and high accuracy rate"[321]. Although the judge was applying these considerations to a case involving sniffer-dogs, they can easily be transposed onto most smart devices as such technology is minimally intrusive[322], specific in nature with a high degree of accuracy.

This was similarly concluded in *R.* v. *Tessling* mentioned previously. In this case, the use of a forward Looking Infra-Red ("FLIR") camera to detect heat, in order to detect drugs, was not a violation of a person's right to privacy. The Court of Appeal found the information inadmissible because the search was done without a warrant. The use of the technology, however, was not a violation of unreasonable search and seizure guaranteed by section 8 of the *Canadian Charter of Rights and Freedoms*, as was the lack of a warrant. The Supreme Court ruled that this type of technology is both non-intrusive and mundane in the data it produced. Thus, it did not violate the

[318] *R.* v. *Edwards,* [1996] 1 SCR 128, 1996 CanLII 255 (SCC), para 33.
[319] *Criminal Code*, R.S.C. 1985, c. C-46, s. 487.
[320] *R.* v. *Vu*, prev. cited, note 137, para. 63.
[321] *R.* v. *A.M.,* [2008] 1 SCR 569, 2008 SCC 19 (CanLII), para 13; 42.
[322] It would be minimally intrusive as such technology can be accessed without the owner's knowledge and without entering a home, it causes minimal inconvenience and it does not interfere with bodily integrity, Lee-Ann CONROD, "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", prev. cited, note 7, p. 127.

defendant's reasonable expectation of privacy as guaranteed in section 8 of the *Canadian Charter*. We could potentially presume that this would be an argument made in favor of using health data in courts, gathered by some smart health technologies. A Fitbit, for example, is both non-intrusive and mundane in the data it produces. The only difference between the latter and a FLIR camera is the user behind the device. Perhaps our right not to incriminate ourselves, as guaranteed by section 13 of the *Canadian Charter*[323], could play in our favor, granted that a warrant is not issued to access our data.

Nonetheless, when accessing sensitive health information, the minimally intrusive nature can be disputed. While accessing data from smart health devices is not as intrusive as other types of searches and can be done by accessing the server where the information is kept, the person whose information is disclosed might want to keep it private as it could be sensitive information revealing a user's lifestyle. Indeed, even if the search is specific in smart health devices, the type of information accessed is sensitive in nature and reveals more about a person than a simple smart bulb, for example. Additionally, once a reasonable expectation of privacy has been established and section 8 becomes applicable, it is a matter of balancing individual interests and the collective desire for security, as well as the public's interest in being left alone and the Government's interest in pursuing law and order by intruding on individual's privacy[324]. Essentially, the best way we see to ensure individual and collective interests, all while respecting section 8 of the *Canadian Charter*, is to require in all cases a judicial pre-authorization, a search warrant, while having reasonable grounds to believe that a crime will be or has been committed and use the information solely granted in the warrant while dismissing the deductable information about the person's lifestyle, sexual orientation, and any data that would unjustifiably violate the right to privacy. Yet, it is also possible to mitigate risks through informed consent.

b) Mitigating the Access of our Information through Consent

The clearest solution to mitigate risks associated with the use of smart health devices is the one that is omitted by many of us: to read the terms and conditions for every contract signed. It is simply impossible to know what rights we are signing away if we have not read the binding

[323] "13. A witness who testifies in any proceedings has the right not to have any incriminating evidence so given used to incriminate that witness in any other proceedings, except in a prosecution for perjury or for the giving of contradictory evidence", *Charte canadienne des droits et libertés*, prev. cited, note 33, article 13.
[324] *Hunter et al*. v. *Southam Inc*., prev. cited, note 315, p. 159.

agreement we blindly accept. Indeed, one of the biggest issues with the use of technology is informed consent such as it was noted by professor GAUTRAIS in *The Colour of E-Consent*[325]. Professor GAUTRAIS defends the position that electronic contracts do not always reflect the actual consent of an individual as they may not always understand the transactions that they are making or the legal rights that they are perhaps unknowingly giving away. From long to unintelligible clauses, there are many reasons why someone would sign away their rights without having much of a choice. Nonetheless, these people, in Quebec, might be protected by sections 1436 and 1437 of the *Civil Code of Quebec*. The question that follows is what happens to our information once we have signed our rights away? It is our right to privacy that is directly affected; the right to keep our personal information confidential. Therefore, it is crucial to fully understand and to read any contract before signing it as it could prevent further problems in regards to keeping personal information confidential. This applies to any contract between a user and their smart health device as such contracts can be numerous when using multiple interconnected devices. They may also be lengthy and unintelligible to the common individual.

However, mitigating the access to our data is not always possible as consent is not always an option. Indeed, at times, to use a specific product or service on a smart health device, a user must consent to the privacy policy of the latter. This minimizes peoples' options in regards to how they can mitigate their risks. Moreover, smart health devices might be required for a specific job or in order to get a better insurance deal such as we have seen with Manulife earlier in the thesis.

Staying on the matter of consent, smart health devices are not restricted to users of a certain age. This means that part of the population using such devices cannot properly consent to their information being gathered, stored and shared amongst third parties. The younger population is beginning to use smart technologies and is accustomed to them since a very young age. Evidently, privacy concerns do arise as information collected on young children is extremely sensitive. Companies cannot gather information on minors; however, seeing that the information is gathered by technologies rather than by humans, distinguishing between which data can be stored and which cannot has its complications. Yet, there is gruesome evidence that some companies like TikTok "illegally collected personal information from children under the age of

[325] Vincent GAUTRAIS, "The Colour of E-Consent", (2004) 1 *UOLTJ* 189-212.

13, such as names, email addresses and their location"[326]. In addition, the app's predecessor Musical.ly collected and exposed the location of young children. This app had failed to comply with demands to delete all information on underage children and was holding onto it longer than necessary. The information collected by the latter included an "email address, phone number, username, first and last name, short bio […] profile picture, […] [and] the child's age, birthdate, or school"[327]. Other companies such as Oath, owned by Verizon, and Disney (DIS) have been fined for collecting and displaying information on minors[328]. This is clearly illegal and a grave preoccupation. These examples are used to demonstrate how companies may willingly gather and share personal data on minors regardless of laws in place. While TikTok videos per se might not reveal sensitive information, wearables used by children and their apps may possibly do so.

In all evidence, children usually are protected, but the fact that they are protected does not change the reality that some of them may take interest in smart health devices containing certain applications and have their information stored. Companies should seek parental consent from minors unable to legally give their consent. Nonetheless, it is not unusual for children to lie about their age, especially when they cannot distinguish right from wrong, which is around the age of 7[329]. Yet, the problem is greater amongst teenagers who seek out age-restricted content. Nonetheless, as noted by the former Privacy Commissioner of Canada (OPC) Jennifer STODDART in 2010, "[t]he average age of children who are on the Internet appears to be dropping, and the implications on their privacy need careful attention from public policy makers. […] Many experts have stated that ensuring children's personal information is protected is an area that needs more attention"[330]. In Quebec, for instance, the age of consent is set at 14, whether it is work-related, for personal leisure, or health-related consent. In addition, people with certain conditions may be unable to properly give their consent such as individuals with special

---

[326] Sherisse PHAM, "TikTok hit with record fine for collecting data on children", *CNN*, February 28, 2019, online: <https://edition.cnn.com/2019/02/28/tech/tiktok-ftc-fine-children/index.html?fbclid=IwAR2yAZMTgHcd8F7dVuM-A8KvtqFKGlaBMb0LNUfd7SZ1ks_xceeTW4QYTLo> (accessed on May 7, 2020).

[327] *Id*.

[328] *Id*.

[329] CURATEUR PUBLIC QUÉBEC, "Les droits du mineur", online : <https://www.curateur.gouv.qc.ca/cura/fr/mineur/tutelle-biens/droits/index.html> (accessed on March 29, 2019).

[330] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", May 2011, online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/report_201105/#fn6> (consulted on March 27, 2020).

needs. This is why it is crucial to enact laws that can protect the data of such people by making sure that whoever is consenting can legally do so and understands the rights they are giving away. As minors take interest in new technologies, including smart health devices, it is important that laws fully protect their privacy while ensuring that third parties are sanctioned for their negligence and respect *PIPEDA*'s accountability principle. Moreover, there should be accountability for "protecting personal information throughout its lifecycle"[331].

Furthermore, as seen earlier in the case of TJX[332], one of the risks of giving away personal information is for such information to be kept and stored longer than needed, if needed at all. While companies on their end should not retain unnecessary personal information nor collect it for longer than necessary, users of smart health devices should make sure that the personal information they consent to give away to third parties will be discarded in a timely manner, when no longer necessary. Indeed, this is stated by Principle 5 of the *PIPEDA*[333].

As well, all data "that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous"[334]. While these were recommendations, the Act still sets the requirement that "[o]rganizations shall develop guidelines and implement procedures to govern the destruction of personal information"[335]. This would reduce the odds of users' personal data from being unwillingly obtained. Thus, one of the solutions to mitigating users' risks comes down to consent and understanding what the consequences in using smart health devices are and what consequences result from sharing personal data with third parties.

Nonetheless, there is a tremendous difference between PII being hacked and it being voluntarily sold or shared to third parties. As for the possibility of PII being sold to third parties, it is

---

[331] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act", 2017, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1> (accessed on July 21, 2020).

[332] *Report of an Investigation into the Security, Collection and Retention of Personal Information*, prev. cited, note 82.

[333] "[o]rganizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods", *Personal Information Protection and Electronic Documents Act*, prev. cited, note 2, Principle 4.5.2.

[334] *Personal Information Protection and Electronic Documents Act*, *Ibid*., Principle 4.5.3.

[335] *Id*., Principle 4.5.3.

important to consult the privacy policy of applications and wearables and to make sure to acknowledge and consent to them before giving away personal data. In fact, the only way to prevent our personal information from being shared to third parties, apart from not having any smart device, is to read the terms and conditions with the privacy policy and to adjust the privacy settings to filter which information we are ready to give away and which information we want to keep private. Nonetheless, the problem can also arise from the hard-to-read policies some company's offer, which can be filled with legal jargon throughout many pages or condensed all on one page[336]. Therefore, privacy policies must be open, transparent and include how the company manages personal data, such as stated in Principle 8 of the *PIPEDA*[337]. The Act also mentions what must be included in the information made available in its Principle 4.8.2.

While the Equifax scandal was a security problem, the Cambridge Analytica scandal was a calculated ethical problem. Facebook puts efforts into avoiding data breaches, yet it voluntarily shares its users' information[338]. These cases can be applied to wearables as the information they collect may "be processed, interpreted, aggregated, stored and shared with others"[339], which can result in a similar privacy issue. The problem, however, is that apart from personal due diligence and controlling as much as possible what information we share, once we share our information with third parties, there is not much a user can do to control where its information goes afterwards, and to whom. As said by security technologist Bruce SCHNEIER in his blog:

> "So while it might be possible for companies to do a better job of protecting our data, you as a consumer are in no position to demand such protection.
>
> Government policy is the missing ingredient. We need standards and a method for enforcement. We need liabilities and the ability to sue companies that poorly secure our

[336] David BURKE, "Why it is important to outsmart the smart devices", prev. cited, note 1.
[337] "[o]rganizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable"*, Personal Information Protection and Electronic Documents Act*, prev. cited, note 2, Principle 4.8.1.
[338] Alix LANGONE, "We Talked to Security Experts About How to Protect Your Online Data. Here's What They Said", *MONEY*, April 17, 2018, online: <https://money.com/how-to-protect-personal-information/> (consulted on March 26, 2020).
[339] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Wearable devices and your privacy", 2017, online: <https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/02_05_d_73_wd/> (accessed on March 27, 2020).

> data. The biggest reason companies don't protect our data online is that it's cheaper not to. Government policy is how we change that"[340].

In Canada, *PIPEDA* would apply to companies such as Facebook, Google and those who produce smart health devices, thus regulating the protection of personal information[341]. In fact, following an investigation by the Office of the Privacy Commissioner of Canada revealing Facebook's violations of privacy laws, many significant changes have been made since then in the company's privacy policies[342]. The Privacy Commissioner of Canada (OPC) Jennifer STODDART, at the time, has even noted that "Facebook has shown greater awareness of users privacy rights […]"[343]. This goes to show that our laws can indeed protect our personal information, even if it is in the hands of foreign organizations located outside of Canada. Facebook is just one case of many to demonstrate that accountability should be enforced whenever possible but also that it can work to better protect user data, especially sensitive data. If accountability is costlier than omission, companies might be willing to better protect user data,

More so, in Canada, under the *PIPEDA*, companies may not collect, use or disclose personal information without the consent and knowledge of the individual to whom it relates[344]. This is

---

[340] Bruce SCHNEIER, "Can Consumers' Online Data Be Protected?", February 14, 2018, online: <https://www.schneier.com/blog/archives/2018/02/can_consumers_o.html> (consulted on March 26, 2020).

[341] Tariq AHMAD, "Online Privacy Law: Canada", prev. cited, note 70; The Privacy Commissioner and the Federal Court of Canada are responsible for enforcing privacy laws in Canada. The Commissioner cannot order compliance, allocate damages, or enforce penalties. However, section 14 (1) of the *PIPEDA* states that "[a] complainant may, after receiving the Commissioner's report or being notified […] that the investigation of the complaint has been discontinued, apply to the Court [Federal Court of Canada] for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report". Moreover, the Federal Court of Canada would then have the authority to order an organization to "correct its practices"; "publish a notice of any action taken or proposed to be taken to correct practices"; and "award damages to the complainant, including damages for any humiliation that the complainant has suffered", such as stated in section 16 of the Act. The Federal Court of Canada has first awarded damages under *PIPEDA* in 2010 in the case of *Nammo* v. *TransUnion of Canada*, [2010] F.C. 1284 (CanLII). This showed the willingness of the Court to award damages in the case of privacy violations. More so, Justice BINNIE said that "[n]ational practice confirms that either the country of transmission or the country of reception may take jurisdiction over a 'communication' linked to its territory […]", *Lawson* v. *Accusearch*, 2007 FC 125 (CanLII), [2007] 4 FCR 314, par 26; *Society of Composers, Authors and Music Publishers of Canada* v. *Canadian Assn. of Internet Providers*, 2004 SCC 45 (CanLII), [2004] 2 SCR 427, par. 68.

[342] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features", April 4, 2012, online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2012/nr-c_120404/> (consulted on March 26, 2020).

[343] *Id*.

[344] Megan EVANS, "A Primer on the Personal Information Protection and Electronic Documents Act ("PIPEDA") for Pharmaceutical and Medical Device/Technology Companies that Conduct Business in Canada", *LONGWOODS*, 2003, online: <https://www.longwoods.com/content/16404> (consulted on March 26, 2020).

seen in principle 3 of the *PIPEDA*. As well, organizations must "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used"[345]. Furthermore, consent must be given by users prior to the collection of their personal data and it should be sought out anew when a new use of their data is identified[346]. Moreover, when an organization seeks consent on sensitive information, such as health data generated by smart health devices, the consent sought out should be express, meaning users should formally agree to the use of their information, in contrast to tacit or implied consent which would be acceptable with less sensitive information[347]. To make sure consent is properly given, organization can follow *PIPEDA*'s suggestions:

> i) Have users fill out application forms to seek consent to collect their information and inform them through such form of the uses they have for users' data. If a user signs this form, they will be giving express consent to the collection and specified uses;
>
> ii) Have users use a checkoff box system where they personally choose which information they do not accept to share with other third parties, such as their names and addresses. If the boxes are left unchecked, this would imply consent for their information to be shared to other third parties;
>
> iii) Consent may be sought out orally, such as by telephone;
>
> iv) Consent may be implied, such as at the moment of use of a product or service[348].

In some cases, consent might not always be required, such are the cases covered in sections 7 (1), 7 (2), 7 (3), 7 (4) and 7 (5) of the *PIPEDA*. Similarly, section 5 (3) states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". This gives rise to a few exceptions that could potentially violate a person's right to privacy. Nevertheless, no exceptions are allowed in regards to sharing and selling personal information for marketing purposes, and most of them tend to benefit the individuals involved.

---

[345] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 2, Principle 4.3.2.
[346] *Id.*, Principle 4.3.1.
[347] *Id*., Principle 4.3.6.
[348] *Id.*, Principle 4.3.7.

If personal information were to be held by the Canadian Government, the *Privacy Act* would also seek individuals' consent. Indeed, consent is covered by section 7[349] and section 8 (1)[350] of the *Privacy Act*. However, consent is not enough by itself to mitigate privacy risks.

c) Mitigating our own Actions

While consent is imperative, it is not the only thing to keep in mind to maintain the safety of personal information. Knowing what information is registered by smart health devices, what is recorded and what can be deduced through it plays a big role in mitigating the risks associated with the safe use of such devices. As said by the Office of the Privacy Commissioner of Canada in a blog, "[y]ou must understand your data before you can protect it!"[351] Indeed, it is important to understand that while a person can have multiple "dumb" smart devices, the information retrieved from every one of them can be put together and provide an accurate representation of someone's profile[352]. Due to the fact that smart devices are usually connected to the Internet of Things and can interact amongst each other, the amount of data recorded can drastically increase with the number of devices used by an individual. As such, someone that owns an Amazon Echo Dot and smart devices compatible with the Echo Dot, such as a smart plug or a smart blub, will have more of their information recorded. This information would include but will not be limited to: all Echo Dot interactions, all browsing history and purchases made on the Amazon website and additionally, all the times the smart plug or smart bulb were used, and when the user leaves the house or goes to sleep, deduced by the latter. The more smart devices connect to each other, the more information can be gathered and revealed. This includes smart health devices that are usually connected to another smart device such as an Apple watch connected to an Iphone.

---

[349] "7 Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except
(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2)."

[350] "8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section."

[351] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know", October 31, 2019, online: <https://www.priv.gc.ca/en/blog/20191031/> (consulted on April 1, 2020).

[352] Kim MILFORD, "December 2019: Get Smart! Mitigating Risks in Connected Devices", *EDUCAUSE*, December 17, 2018, online: <https://er.educause.edu/blogs/2018/12/december-2019-get-smart-mitigating-risks-in-connected-devices> (accessed on March 24, 2020).

The increased interoperability between smart devices increases the number of potential vulnerabilities. Indeed, when smart health devices connect to a home network, Wi-Fi or a cellphone network and are transmitted to a health professional, the data transmitted becomes prone to hacking and the privacy of the users becomes at risk[353]. As shown earlier, hacking is one of the risks associated with smart devices connected to the Internet of Things (IoT). It is a greater risk if the information generated by smart devices is health related because, as we have seen, it is highly in demand by cybercriminals who seek to sell it or to profit from it through identity theft. As well, there are also health risks if the hackers are able to stop a smart health device from functioning, such as a pacemaker or a heart rate monitor. More so, this same data desired and used by cybercriminals is also of value to third-parties who seek to sell this information and profit from it through marketing. Indeed, there are industries that profit from selling personal health information generated by applications and wearables which provide "real-time data on geolocation, activities, and behavioral patterns"[354].

Fortunately, there are a few things users of these devices can do to mitigate such risks. We shall name a few as suggested by Norton security software. Just as computers require regular updates to patch security holes[355], every generation of wearables comes with newer and more sophisticated security features[356]. This means that while it may be costlier, it would be safer to invest in newer generations of smart health devices than to opt for a previous and cheaper model. These devices should also be updated when possible. Furthermore, it would be important to let smart devices have access to only the most critical information needed for usage. While it is possible in some cases to manage the information applications on smart devices have access to, it is also suggested to reduce storing in such devices any critical personal information such as your Social Security number, bank accounts, credit card information, and your home address. Thus, if a user of smart health devices shops online, they ought to refrain from doing so through

[353] DELOITTE CENTRE FOR HEALTH SOLUTIONS, "Medtech and the Internet of Medical Things | How connected medical devices are transforming health care", prev. cited, note 188, p 22.
[354] Kenneth R. FOSTER and John TOROUS, "The Opportunity and Obstacles for Smartwatches and Wearable Sensors", prev. cited, note 183.
[355] The Equifax data breach is a perfect example of a failed attempt by a company to update its software, resulting in the theft of personally identifiable information of around 143 million Americans. The information retained consisted of Social Security numbers, dates of birth, and home addresses; Gary DAVIS, "Why Software Updates are so Important", *MCAFEE*, September 17, 2017, online: <https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important/> (consulted on March 26, 2020).
[356] NORTON, "How to protect your connected wearables", online: <https://ca.norton.com/internetsecurity-iot-how-to-protect-your-connected-wearables.html> (consulted on March 26, 2020).

wearables. However, when using smart health devices that required data or internet connectivity, users should refrain as much as possible from connecting to public Wi-Fi. Hackers can position themselves between users of smart devices and the connection point which enables the hackers to receive the users' information instead of it being sent to the hotspot. Hackers then receive every information sent out such as emails and personally identifiable information (PII)[357]. Therefore, making sure all personal devices are connected through data rather than Wi-Fi, or even Bluetooth, would increase the protection of PII.

There are also a few more things users of smart health devices can do on their own to reduce the risks associated with the use of these devices. While we have discussed the possibility of these devices turning against their users, risks associated with subpoenas cannot be mitigated and are simply to take into account in considering whether the benefits of sharing personal data to benefit overall health exceed the risks associated with it[358].

The main solution comes down to understanding what information is gathered and what can be deduced by personal smart health devices and how this information can turn against the users or negatively impact them. Smart devices can indeed be used in trials, but when such devices are permitted or requested, the data they register has to be unedited and raw such as seen in *Benisty* c. *Kloda*[359]. Hence, it would not be possible to eliminate undesired pieces of data from evidence and the metadata in smart devices would reveal more information than anticipated. However, in the case of a subpoena following a warrant, only the information part of the search should be admissible and taken into consideration. Yet, we see that this is not always the case when evidence obtained illegally can be used after assessing the impact on the administration of justice. It might seem that in any case, when personal information is obtained through legal means, users of devices from which the data is retrieved are in a disadvantage. However, this does not mean that they cannot reduce the risks deriving from the access to their information.

---

[357] Justin DOLLY, "Why you should never, ever connect to public WiFi", *CSO*, January 9, 2018, online: <https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html> (consulted on March 26, 2020).

[358] As shows earlier, *PIPEDA* allows for personal data to be shared without users' consent in some circumstances. Personal data can therefore be "required to comply with a subpoena or warrant issued or an order made by a Court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records", *Personal Information Protection and Electronic Documents Act*, prev. cited, note 2, section 7 (3) (c).

[359] *Benisty* c. *Kloda*, 2018 QCCA 608 (CanLII).

First and foremost, users of smart devices are in control of which device they use and what information they allow to share with them, to a certain extent. They key word is control. Essentially, it is a matter of having control over one's gadget, instead of it having control over you. Thus, one way of taking back control is limiting the amount of smart devices and keeping the essentials, which in most cases would be smart health devices, and then again, not all of them. Indeed, while a video doorbell sounds convenient, it poses concerns in terms of privacy. As an example, the police has partnered up with Amazon to be able to "download videos captured by homeowners' Ring doorbell cameras […] keep them forever and share them with whomever they'd like without providing evidence of a crime"[360]. This being said, if a user's goal is to count steps in a day, a Fitbit would be a better option than a smart watch as the latter would compute a greater amount of information on the user. Thus, keeping only the essential smart health devices is a way to take control over how much information is gathered on oneself. Additionally, not every smart device needs to be one. We have mentioned that there are "dumb" smart devices such as refrigerators, kettles and household appliances. While they are convenient, having many smart devices connected to the Internet of Things increases the data generated and potential vulnerabilities. While such data is benign on its own, it may reveal a lot about its user when added to a conglomerate of data derived from many devices. Therefore, owners of smart health devices whose sensitive information is already computed should refrain from using other smart devices that are non essential and avoid exposing themselves to greater privacy risks.

Secondly, while going back to the matter of consent, it is important to take the time to properly consent, or not, to the different types of data collection presented by smart devices. It can be easy to run through them in anticipation of using the devices as soon as possible; yet, taking the time to read through what one is consenting to can significantly reduce the risks in terms of privacy. It is, in fact, important to know what data is collected, which part of it is public and what apps can access personal information. Apart from privacy policies, it can be suggested to consult settings, sharing and storage options along with what will be accessed by an application when in use. Most times, applications in smart devices request access to a user's camera, contacts, and other personal information to properly function. While some accesses are essential for an application's

[360] Drew HARWELL, "Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator", *THE WASHINGTON POST*, November 19, 2019, online: <https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/> (accessed on March 27, 2020).

functionality, others can be denied which would reduce the amount of data stored by some apps. Users should also control what information can be visible to others. Other times, it can be possible to change what information is being collected through default settings because they can be geared towards collecting and sharing personal data. The same goes for smart wearable devices. Wearables should be configured to maximize privacy[361]. It would also benefit the users to seek out if manufacturers of their devices follow any security or privacy standards or certifications such as International Standards Organization (ISO) norms. Essentially, the more access is provided, the more information is compiled.

Thirdly, it is possible to limit the amount of data collected by shutting off smart devices that are not currently in use. Some devices such as a Fitbit calculate the number of steps taken in a day. Unless a user is a sleepwalker, there would be no need to keep the device on during the night. In fact, the Fitbit can register the amount of times a person has been inactive, hence in bed, through the constant usage of this device[362]. Moreover, in the event that a user decides to cease using one of their devices permanently, they should ensure that all their data is permanently removed from the devices, which sometimes involves following more steps than simply resetting a device to its factory settings. If wiping away the memory is not possible, the memory chip should be destroyed[363].

In essence, following these suggestions would reduce the amount of data generated and the amount of smart devices used, leaving users with mostly smart health devices as these can be considered essential in some cases. However, relying too much on smart health devices can also cause problems of its own. In fact, the use of these inexpensive off-the-shelf wearables can create distress and fear through false positives. While these devices do a good job in preventing numerous health problems, with all the data generated, it may lead to overdiagnosis, especially in asymptomatic individuals[364]. The amount of false positives may be overwhelming for the users

---

[361] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Wearable devices and your privacy", 2017, online: <https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/02_05_d_73_wd/> (accessed on March 27, 2020).

[362] Francisco de ARRIBA-PÉREZ, Manuel CAEIRO-RODRIGUEZ and Juan M. SANTOS-GAGO, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", prev. cited, note 119, point 4.1.

[363] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Wearable devices and your privacy", *Ibid*.

[364] Kenneth R. FOSTER and John TOROUS, "The Opportunity and Obstacles for Smartwatches and Wearable Sensors", prev. cited, note 183.

of smart health devices along with the medical community. However, while it could be dangerous for a consumer to self-diagnose and seek treatment by themselves, it could be fatal to ignore unusual health diagnostics and symptoms. Smart health devices should never replace personal judgment in regards to one's state of health, but they should serve as an additional tool in monitoring symptoms that the body does not recognize as warning signs yet.

Thus, in order to use smart health devices to monitor health aberrations, it is crucial for users to protect themselves from privacy breaches, but this responsibility also falls onto the Government.

2. The Government

a) Mitigating the Gaps in Privacy Management: Hacking Risks in Healthcare and Privacy Laws

As discussed in the risk section, the Government and its institutions might face the risk of unauthorized seizure of PII as seen in the case of the WannaCry ransomware, amongst other similar incidents. This is especially true if the solution of a national database generated by the data of countless individuals by means of smart health devices comes to fruition. Therefore, governments and health facilities must find ways to protect personal health information from hackers and from those who wish to profit from it by mitigating this risk. Yet, it is not solely the Government's role to mitigate risks in the health field; it is also every healthcare provider's responsibility to ensure that they are taking the necessary steps to avoid future attacks.

Indeed, cybersecurity often falls as a last priority in healthcare institutions[365]. This is because cybersecurity does not generate revenue and health organizations usually prefer investing their money on research, equipment and on new technologies to enhance the quality of patient care and of services provided. This leads to other problems such as understaffing of IT professionals and not having enough training for healthcare staff. Other times, the problem comes from the source, which means it can come directly from third parties who create health apps or smart health devices. In fact, healthcare software can only be produced by the vendor and not by healthcare facilities[366]. This could create a delay in maintenance and patching up flaws in the system. If the latter are not dealt with in a timely manner, the systems will be vulnerable to exploitation and it could lead to a breach, leaving numerous personally identifiable information

[365] CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", prev. cited, note 167, p. 29.
[366] *Id*.

available to hackers. If these same health devices are to be used to compute and generate data for a national database, such risks should be dealt with beforehand. Thus, a greater part of the Government's budget could be allocated towards healthcare facilities for them to invest in IT and into proper training. As for the use of smart health devices in generating health data for a national database, only trusted, secure and up-to-date wearables and applications should be allowed. The keepers of the database itself should be weary of potential hacking risks and flaws in the system, especially that PHI would be located on the national and international level at the World Health Organization. However, due to the anonymity concept within the database, hacking would not be much of an issue unless the hackers are able to retrace the information back to specific individuals, which could be possible. The Government should therefore focus on the transmission of data between wearables and the database and between smart health devices and healthcare facilities that use them. The solution for the latter could be to allocate more funding in risk protection management. As for the transmission of data between wearables and the database, a barrier could be created between the data and third parties through network segmentation, which means splitting the network into subnetworks[367].

Moreover, due to the fact that some provinces in Canada have enacted their own privacy laws, there are discrepancies in Canadian laws on the right to know if your data has been breached. Under *PIPEDA*, every data breach must be reported, amongst other requirements. Yet, while the *PIPEDA* offers a reasonable protection in this regard now, it did not come without flaws. A report[368] dating back to May 2013 by the Office of the Privacy Commissioner of Canada noted numerous shortcomings in the current legal system and called for a reform of the *PIPEDA*[369].

---

[367] CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", prev. cited, note 167, p. 30.
When a network is segmented, it is divided into numerous smaller networks which function through small networks called subnet. The flow of traffic can be controlled between subnets. This means that it is possible to grant, restrict or even block access to some subnets based on a variety of factors. Network segmentation can increase a network's performance because it will contain the traffic to the portions of the network that could be seen. It can also localize technical issues with greater ease. This can also prevent unauthorized network traffic or attacks in the areas of the network that contain more sensitive information. Monitoring traffic is also easier through this segmentation.
See: Jason ANDRESS and Mark LEARY, "Protect the Data – Chapter 6", in *Building a Practical Information Security Program*, Syngress, 2015, pp. 103-123, on p. 115, <https://www.sciencedirect.com/topics/computer-science/network-segmentation>.

[368] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Case for Reforming the Personal Information Protection and Electronic Documents Act", May 2013, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/pipeda_r/pipeda_r_201305/>.

[369] Florimond ÉPÉE, "La protection des données personnelles au Canada à l'ère des données massives", prev. cited, note 52.

Some of the problems were that there was a lack of power to impose administrative sanctions, opacity regarding the data transmitted by companies to public authorities, and a difficulty in engaging corporate responsibility when the latter are found to be responsible for a breach in the protection of personal data. The *PIPEDA* has since been amended, following the Equifax scandal[370], and obliges companies since November 1, 2018 to report to the Office of the Privacy Commissioner of Canada the occurrence of any data breach, to keep records of every breach for a minimum of two years[371] and to notify affected individuals at risk[372]. *PIPEDA* also set out important guidelines to ensure that individual consent is given when accessing personal information, namely colleting, using or disclosing it. Such is the case in Principles 4.3 and 4.3.6 of the Act[373]. This is very important progress in terms of the protection of personal information because the citizens of Canada now have to be informed whenever their personal data is accessed without their consent. This does not diminish the risk associated with the availability of personal information to third parties or other entities, but it provides transparency as to what happens to this information in the hands of others.

Notwithstanding this progress, not all provinces have the same requirements. For example, Alberta was the only Canadian jurisdiction to have had a mandatory breach notification regime in place prior to *PIPEDA* amendments of 2018[374]. This allowed the province to take action against a privacy breach from Uber Canada in 2016 who put at risk the personal information of over 800,000 Canadians and waited a year before notifying the affected individuals[375]. Precisely, as stated in section 34.1 (1) of the *Personal Information Protection Act*:

---

[370] David SHIPLEY, "Equifax data breach a 'digital disaster' for Canadians", *CBC NEWS*, September 17, 2017, online: <https://www.cbc.ca/news/canada/new-brunswick/nb-opinion-equifax-data-breach-1.4293609> (accessed on October 27, 2019).

[371] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know", prev. cited, note 351.

[372] Florimond ÉPÉE, "La protection des données personnelles au Canada à l'ère des données massives", prev. cited, note 52.
Also see: Adam KARDASH and Patricia KOSSEIM, "Canada", in *The International Comparative Legal Guide to: Data Protection 2018*, London, Global Legal Group, 2018, p. 54, on page 62.

[373] *Use of sensitive health information for targeting of Google ads raises privacy concerns*, 2014 CanLII 3357 (PCC), para. 20-22.

[374] Mark E. FANCOURT-SMITH, "Mandatory Data Breach Notification Regime Announced Amid Facebook Scandal", *LAWSONLUNDELL*, April 13, 2018, online: <https://www.lawsonlundell.com/Commercial-Litigation-and-Dispute-Resolution-Blog/mandatory-data-breach-notification-regime-announced-amid-facebook-scandal> (consulted on April 1, 2020).

[375] *Id*.

> "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure"[376].

This means that private and public organizations that hold personal data must report data breaches that can cause a real risk of significant harm. They must also inform the individuals who had their data breached, report to the Privacy Commissioner and to the Minister of Health[377]. There is also a mandatory breach reporting requirement under section 60.1 (1) of *Alberta's Health Information Act* (HIA)[378] in regards to the public health sector. As well, Ontario, New Brunswick and Newfoundland and Labrador also have reporting requirements in their provincial health privacy laws. On the contrary, in British Columbia, public bodies do not have the obligation to report data breaches to individuals nor to the Privacy Commissioner, even if it is health data; data that could be generated by smart health devices. Indeed "PIPA does not currently require mandatory reporting, but complying with the federal law is considered best practice […]"[379]. Quebec has also not yet introduced breach notification requirements in its legislation but Quebec's former minister of justice was considering introducing a bill to modernize its provincial privacy regime. The changes would include:

> "(i) tighter rules governing the consent of persons concerned, (ii) the possibility for these individuals to withdraw their consent and the company's obligation to destroy their personal information it holds, (iii) the obligation for the company to report any security

---

Also see: THE CANADIAN PRESS, "Uber to inform Canadians affected by data breach Social Sharing", *CBC*, March 9, 2018, online: <https://www.cbc.ca/news/business/uber-breach-data-canadians-1.4570507> (consulted on April 1, 2020).

[376] *Personal Information Protection Act*, prev. cited, note 63.

[377] Birch MILLER and de Lobe LEDERMAN, "Cybersecurity Data Breaches and Mandatory Privacy Breach Reporting: Lessons from Alberta", *BLAKES*, October 18, 2016, online: <https://www.blakes.com/insights/bulletins/2016/cybersecurity-data-breaches-and-mandatory-privacy> (consulted on April 1, 2020).

[378] "60.1(1) Subject to the regulations, an affiliate of a custodian must as soon as practicable notify the custodian in accordance with the regulations of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian."
Health Information Act, S.A. 2018, c. H-5.

[379] BEACON LAW CENTER, "New Data Breach Reporting Rules", March 29, 2019, online: <https://beaconlaw.ca/new-data-breach-reporting-rules/> (consulted on April 1, 2020).

> incident, including loss of data, (iv) increased powers granted to Quebec's access to information commission and higher applicable penalties, and (v) the Act's expanded scope of application to public bodies"[380].

As a matter of fact, Quebec's legislation protecting personal information had been adopted in the 1990's and has not been significantly updated since[381]. In September 2019, Quebec's then minister of justice Sonia LEBEL said that the new bill she was working on would also seek to regulate the protection of personal data in public and private matters and also concerning the management of personal data by political parties[382]. The latter is extremely important and would contribute greatly towards mitigating data protection risks as political parties are exempt from "privacy laws that regulate the storage, collection and use of personal information" and they do not have to report to the OPC nor to individuals of any data breaches[383]. If political parties got a hold of the data produced by smart health devices, it could further violate citizens' right to privacy. Moreover, the federal government has to report certain data breaches but there are still no laws mandating political parties and some provincial public bodies to report such breaches, whether to individuals or to the OPC. Creating accountability for these entities would be a step towards safer data management as "[p]ublic agencies have some of the most sensitive information on Canadians including financial data, medical information and even how you voted"[384]. If the Government were to create a national database generated by smart health devices, it would indeed have access to the medical information of its citizens and other unaccounted for data aggregated by such devices. This is why this step forward towards accountability by public agencies is crucial. As said by Kevin NEWMAN in a podcast, "health authorities in British Columbia are entrusted with the most sensitive information about a person

---

[380] Dominic DUPOY and Julie HIMO, "New privacy legislation could increase the burden for companies in Quebec", *DATA PROTECTION REPORT*, February 24, 2020, online: <https://www.dataprotectionreport.com/2020/02/new-privacy-legislation-could-increase-the-burden-for-companies-in-quebec/> (consulted on April 1, 2020).

[381] Mylène CRÊTE, "Québec déposera un projet de loi sur la protection des données personnelles", *LE DEVOIR*, September 18, 2019, online : <https://www.ledevoir.com/politique/quebec/562810/quebec-deposera-un-projet-de-loi-sur-la-protection-des-donnees-personnelles> (consulted on April 2, 2020); LANGLOIS AVOCATS, "2020 : l'année des modifications aux lois canadiennes et québécoises sur la protection des renseignements personnels", January 21, 2020, online : <https://langlois.ca/2020-lannee-des-modifications-aux-lois-canadiennes-et-quebecoises-sur-la-protection-des-renseignements-personnels/> (consulted on April 2, 2020).

[382] Mylène CRÊTE, "Québec déposera un projet de loi sur la protection […]", *Ibid*.

[383] Francesca FIONDA, "19 million Canadians have had their data breached in eight months", *CTV NEWS*, September 2, 2019, online: <https://www.ctvnews.ca/politics/19-million-canadians-have-had-their-data-breached-in-eight-months-1.4572535> (consulted on April 2, 2020).

[384] *Id*.

that you can possibly imagine, and so the responsibility to make sure it is properly secured is a significant bar they need to ensure that they meet"[385]. It is also revealed in this podcast that it is obscure what public bodies and political parties do with our data which means a stricter monitoring should be envisioned to cover them and what they do with our personal information.

Thus, it would be important to have uniformity in privacy laws amongst all Canadian provinces to avoid gaps within it; at least when it comes to the principles set by the *PIPEDA*, in particular the accountability one. While we acknowledge the provincial right to legislate based on the division of powers, we believe that personal health data should be protected equally, at the same standards set by the *PIPEDA*, regardless of the location of this information. Accountability is therefore an important principle to abide by, whether it is for data transfer or disclosure of data breaches.

It is to note that out of the 446 breaches reported to the OPC between November 2018 and June 2019, affecting around 19 million Canadians, 59% of them were due to hacking, 22% were due to accidental disclosures, 13% resulted from a loss of data and 6% was from physical theft[386]. To cope with some of the risks association with the use of technology, Minister of Innovation, Science and Economic Development Navdeep BAINS announced the creation of Canada's new Digital Charter on May 21, 2019[387]. This Charter is filled with proposals aimed to modernize *PIPEDA*. The 10 principles of the Charter will consist of: universal access[388]; safety and security[389]; control and consent[390]; transparency, portability and interoperability[391]; open and

---

[385] Kevin NEWMAN, "Rooftops, Radio Waves & Your Health Data", in *Attention Control with Kevin Newman*, *APPLE PODCASTS*, September 9, 2019, at 18:50, online: <https://podcasts.apple.com/ca/podcast/rooftops-radio-waves-you/id1476566791?i=1000449085670> (consulted on April 2, 2020).

[386] Francesca FIONDA, "19 million Canadians have had their data breached in eight months", prev. cited, note 383.

[387] GOVERNMENT OF CANADA, "Canada's Digital Charter: Trust in a digital world", June 25, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html> (consulted on April 2, 2020).
Also see: GOVERNMENT OF CANADA, "Minister Bains announces Canada's Digital Charter", May 21, 2019, online: <https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/minister-bains-announces-canadas-digital-charter.html> (consulted on April 2, 2020).

[388] "All Canadians will have equal opportunity to participate in the digital world and the necessary tools to do so, including access, connectivity, literacy and skills." GOVERNMENT OF CANADA, "Canada's Digital Charter: Trust in a digital world", *Id*.

[389] "Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online", *Id*.

[390] "Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected", *Id*.

[391] "Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden", *Id*.

modern digital government[392]; a level playing field[393]; data and digital for good[394]; strong democracy[395]; free from hate and violent extremism[396] and strong enforcement and real accountability[397]. Government policies and legislation will be measured against these principles. The latter will allow Canadians to have more control over their data and to know how their data is being used and by whom[398]. Indeed, the Government has already committed to revising the *PIPEDA* to make sure it is consistent with the Digital Charter[399]. Some of the changes we might expect to see, based on the new Charter, would be in regards to "data mobility, online reputation, consent, oversight and enforcement"[400]. The Government has released a discussion paper aimed at sharing Canadians' concerns regarding their privacy and how to modernize *PIPEDA* based on them and the Digital Charter[401]. Canada's federal private-sector privacy regime would seek to achieve the outcomes related to the principles set by the new Charter. This would in turn allow individuals to have more control over their personal data while avoiding burdensome restrictions for businesses. Moreover, the Government of Canada proposed

> "clarifications under PIPEDA that detail what information individuals should receive when they provide consent; certain exceptions to consent; data mobility; deletion and withdrawal of consent; incentives for certification, codes, standards, and data trusts;

---

[392] "Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use", GOVERNMENT OF CANADA, "Canada's Digital Charter: Trust in a digital world", prev. cited, note 387.

[393] "The Government of Canada will ensure fair competition in the online marketplace to facilitate the growth of Canadian businesses and affirm Canada's leadership on digital and data innovation, while protecting Canadian consumers from market abuses", *Id*.

[394] "The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people—at home and around the world", *Id*.

[395] "The Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions", *Id*.

[396] "Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content", *Id*.

[397] "There will be clear, meaningful penalties for violations of the laws and regulations that support these principles", *Id*.

[398] Alex BOUTILIER, "New 'digital charter' to emphasize Canadians' control over personal data", *THE STAR*, May 21, 2019, online: <https://www.thestar.com/politics/federal/2019/05/21/new-digital-charter-to-emphasize-canadians-control-over-personal-data.html> (accessed on April 6, 2020).

[399] Keri L. BENNETT and Jordan MICHAUX, "Canada: Canada's Digital Charter: The Problem Of Trust In A Growing Digital World", *MONDAQ*, June 19, 2019, online: <https://www.mondaq.com/canada/Privacy/816656/Canada39s-Digital-Charter-The-Problem-Of-Trust-In-A-Growing-Digital-World> (accessed on April 6, 2020).

[400] *Id*.

[401] GOVERNMENT OF CANADA, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians", October 23, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html> (accessed on April 6, 2020).
Also see: GOVERNMENT OF CANADA, "Strengthening Privacy for the Digital Age", May 21, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html> (accessed on April 6, 2020).

> enhanced powers for the Office of the Privacy Commissioner; as well certain modernizations to the structure of the law itself and various definitions"[402].

Changes to this Act would have to be reflected in provincial legislations which were deemed substantially similar to *PIPEDA*; however, until then, it would be important for the three provinces concerned not to fall behind in regards to the protection of personal data, such as it was done in British Columbia and in Quebec. Some reforms are also to be expected in regards to the *Privacy Act*[403]. After all, it is in the Government's advantage to maximize data protection to get citizens' trust, especially if it were to follow suit with the idea of creating a national database. Indeed, as we will demonstrate below, the Government and the users of smart health devices can favor their advantages through the creation of a national and international database which could help improve public health by preventing and tackling diseases as they arise.

B. Favoring the Advantages of Smart Health Devices

Having covered some of the ways both users and the Government can mitigate the risks of using smart health devices whether for personal use or in healthcare, we shall now explain how the latter can favor their advantages through the creation of a national and international database. We believe that a more accurate surveillance of upcoming diseases and viruses, whether it is done by State or supra-State bodies, can improve a population's overall health.

1. How the Government(s) and the WHO Would Benefit From a Database and its Establishment

a) Benefiting from a Database Generated by Smart Health Devices

Our personal health data can be our weakness but also our strength. This is why it is crucial to reform the healthcare system by increasing the use of smart devices in healthcare. At the present moment, the federal government does not collect the information about individuals' health as it stays confidential between a physician and its client, unless consent is provided to disclose such data, such as previously seen in the *PIPEDA*. Moreover, every province and

[402] GOVERNMENT OF CANADA, "Strengthening Privacy for the Digital Age", prev. cited, note 401.
[403] GOVERNMENT OF CANADA, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians", prev. cited, note 401.

territory has its own distinct health system for which it is responsible for[404]. This is due to the division of powers between the federal and the provincial governments. When the Constitutional Act of 1867[405] was enacted, health was not expressly attributed to one or the other Government in sections 91 and 92. Later on, in 1982, the Supreme Court of Canada declared that

> "[h]ealth is not a subject specifically dealt with in the Constitution Act either in 1867 or by way of subsequent amendment. It is by the Constitution not assigned either to the federal or provincial legislative authority. Legislation dealing with health matters has been found within the provincial power where the approach in the legislation is to an aspect of health, local in nature. […] On the other hand, federal legislation in relation to "health" can be supported where the dimension of the problem is national rather than local in nature […], or where the health concern arises in the context of a public wrong and the response is a criminal prohibition"[406].

On the one side, this is convenient for tailoring particular health services needed for the residents of a specific area. On the other side, the coordination of health reforms becomes challenging and we see an opportunity to gather all health data at the federal level through a centralized server accessible by both levels of the Government for which the Public Health Agency of Canada would be responsible for. The objective would be to allocate resources efficiently to problematic areas in the country or to make policies ensuring appropriate healthcare needs are met everywhere, amongst the first nation people and the citizens. We would like to push this idea further by suggesting an international health database at the World Health Organization such as the Global Health Observatory (GHO)[407] but fuelled by the inputs of smart health devices. If brands such as Apple could partner with the WHO, along with the cooperation of all governments, then it would be possible to track and even predict future epidemics based on live inputs generated at a global scale. Although this is already done to some extent, it has not yet reached its full potential. Indeed, similar partnerships could be made such as it was done with

---

[404] Kathleen O'GRADY and Noralou ROOS, "Five things Canadians get wrong about the health system", *THE GLOBE AND MAIL*, September 5, 2014, online: <https://www.theglobeandmail.com/opinion/five-things-canadians-get-wrong-about-the-health-system/article20360452/> (consulted on October 8, 2019).
[405] *Loi constitutionnelle de 1867*, 30 & 31 Vict., c. 3 (R.-U.).
[406] *Schneider* v. *The Queen,* [1982] 2 SCR 112, 1982 CanLII 26 (SCC), p. 141.
[407] WORLD HEALTH ORGANIZATION, "Global Health Observatory (GHO) data", online: <https://www.who.int/gho/en/> (accessed on October 28, 2019).

Google through "the Google Fit app"[408]. Moreover, during the Seventy-first World Health Assembly held on May 26, 2018, governments saw the true benefits of smart health devices by recognizing that they can "improve public health, promote universal health coverage and advance the Sustainable Development Goals"[409]. As countries have an obligation of helping each other[410], they could do so by exchanging technologies for skills, information or other desired goods, resulting in a win-win situation instead of a rivalry between them in the hopes of balancing their power. It would also benefit all countries because health issues are not country bound. Therefore, cooperation is necessary to ensure that diseases and epidemics do not spread worldwide. This was also acknowledged during the World Health Assembly. Additionally, it would greatly benefit the WHO as it has been criticized for its slow reactions to epidemics and its capacity to adapt to a fast changing environment, namely being criticized for the slow reaction during the Ebola epidemic of 2013-2015 in West Africa that caused 11,300 deaths[411]. Although the international organization has made progress since, it needs to further work on prevention methods and means to control epidemics onsite, especially with the rise of new viruses such as the novel coronavirus mentioned above. As a matter of fact, following this pandemic, the WHO has been severely criticized, even more than before[412]. As a solution, the WHO could make recommendations to its Member States to invest in smart health devices to help control the progression of health conditions in affected or at risk communities. While controlling diseases such as Ebola would be a long shot, it would be efficient in controlling obesity, one of the main health issues addressed by the World Health Organization[413]. If the effects of the database are greater than anticipated, it would already be an improvement to the current situation.

Indeed, greater protections are increasingly important as our solution slowly comes to fruition. The Government seems to support the idea of using wearables and other smart devices in

---

[408] WORLD HEALTH ORGANIZATION, "Digital health", online: <https://www.who.int/behealthy/digital-health/promoting-health-in-the-21st-century> (accessed on October 28, 2019).
[409] WORLD HEALTH ORGANIZATION, *Id*; *The Seventy-first World Health Assembly*, Res. WHA71.7, (May 26, 2018), online: <http://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf> (accessed on October 28, 2019).
[410] *International Health Regulations (2005)*, prev. cited, note 289, article 44.
[411] AGENCE FRANCE-PRESSE, "Ebola : la réaction rapide de l'OMS saluée, mais bémol sur la prévention", *RADIO-CANADA*, May 25, 2018, online : <https://ici.radio-canada.ca/nouvelle/1103282/ebola-reaction-rapide-oms-saluee-prevention-critiquee-organisation-mondiale-sante-virus-vaccin> (accessed on October 28, 2019).
[412] Stephen BURANYI, "The WHO v coronavirus: why it can't handle the pandemic", *THE GUARDIAN*, April 10, 2020, online: <https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-v-coronavirus-why-it-cant-handle-pandemic> (consulted on April 24, 2020).
[413] WORLD HEALTH ORGANIZATION, "Obesity and overweight", February 16, 2018, online: <https://www.who.int/news-room/fact-sheets/detail/obesity-and-overweight> (accessed on October 28, 2019).

healthcare in its approach to digital health technologies and believes that such devices have the "potential to make the delivery of health care more accessible, convenient and cost-effective"[414], as noted previously. In addition, the Government believes that these "technologies can improve access to health care information, facilitate more timely diagnoses and treatments, and improve access to care for patients at home, at health care facilities, as well as in rural and remote communities". More so, "Health Canada expects that this initiative will benefit Canadian patients and the health care system by improving access to innovative digital health technologies that have rapid development cycles while potentially saving health care system costs"[415]. As for enhancing legal protections, the OPC commissioner suggests that:

> "Legislation should define privacy in its broadest and true sense, […] by describing it as freedom from unjustified surveillance. Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. Legislation should recognize and protect their freedom to live and develop independently as persons, away from the watchful eye of a surveillance state or commercial enterprises, while still participating voluntarily and safely in the regular, day-to-day activities of a modern digital society"[416].

The Government should also only collect data "necessary for [the] operation of a program or activity and proportional to the privacy risks"[417]. Hence, there are privacy reform plans to modernize *PIPEDA* and the *Privacy Act*. Moreover, third parties are also willing to cooperate. As a matter of fact, since the COVID-19 pandemic, we are seeing how third parties owning some of the biggest smart device name brands are willingly cooperating with public health officials to help them track the spread of the Coronavirus[418]. Fitbit users are able to participate in studies through the company's COVID-19 Resource Hub. Apple and Google have also announced plans "to develop API-enabled interoperability between iOS and Android products – and eventually build Bluetooth-based contact-tracing functionality into their respective operating systems"[419] to track the spread of the virus. As said by Dr. Eric TOPOL, director and founder of SRTI: "From

---

[414] GOVERNMENT OF CANADA, "Notice: Health Canada's Approach to Digital Health Technologies", April 10, 2018, online: <https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html> (accessed on May 18, 2020).
[415] *Id*.
[416] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Law Reform […]", prev. cited, note 156.
[417] *Id*.
[418] Mike MILIARD, "Scripps, Stanford working with Fitbit […]", prev. cited, note 253.
[419] *Id*.

our previously published work, we know that data collected from consumer wearables can significantly improve the prediction of influenza-like illness"; he sees "an enormous opportunity to enhance disease tracking for improved population health during the COVID-19 pandemic"[420].

Indeed, Apple and Google added features to their mobile operating systems making it possible for certain apps monitored by Government agencies to use Bluetooth to track the proximity between phones in order to identify who has been in contact with a coronavirus carrier[421]. The way this works is if a carrier is positively diagnosed with the virus, they can report it through the app and the latter will inform anyone who has been in proximity to the carrier through a notification. Evidently, this poses privacy concerns for many, mainly concerns regarding the possibility for COVID-19 users to be revealed. Since the contact tracing solution requires access to users' location, this could potentially be used as incriminating evidence as seen previously in insurance scams, criminal misconduct or abuse of work leave days. We could also assume that in the case of a criminal activity, such techniques could also be used to track people who were in proximity to a criminal, hence violating their right to privacy, even if they were innocent. Not to mention that this "can be used as evidence of everything from extramarital affairs to political dissent"[422]. Thus, *PIPEDA*'s accountability principle should be enforced to prevent third parties from unjustifiably violating users' privacy[423]. Yet, if this works with certain apps, it could work on other health apps connected to smart health devices and equally benefit the Government. This said, while we see the clear benefits and feasibility of smart devices used to improve overall health, and while we also have the willingness of the Government and third-parties to cooperate with health officials to diagnose and prevent the spread of diseases, we nonetheless acknowledge the many privacy concerns that may persist if laws do not properly protect individuals' privacy.

b) How the Database Works

In order to understand how the database will work, it is important to understand what was already done and what can be done. In September 2019, Apple launched a new Research app that

---

[420] Mike MILIARD, "Scripps, Stanford working with Fitbit […]", prev. cited, note 253.
[421] Andy GREENBERG, "Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered", *WIRED*, April 17, 2020, online: <https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/> (accessed on May 18, 2020).
[422] *Id*.
[423] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy", prev. cited, note 156.

will work with all Apple Watch users in the United States and will allow them to contribute to health research by sharing the personal health information collected by the smart device through its sensors[424]. This will work through private contributions by the users to several new health studies in collaboration with the World Health Organization, amongst other partners. The data extracted from the Smart Watch could potentially reveal "the long-term effects of sounds on your hearing health; how menstrual cycles can inform the screenings for infertility and osteoporosis; and how activity and movement impacts overall health"[425]. This data allows researchers to conduct studies on a larger scale and in ways that were not possible previously. Before the release of the new Research app by Apple, such health studies were both costly and time consuming. With its release and opt-in option for sharing personal health data such as the heart rate, the motion and activity level along with sound exposure, it is allowing for a quicker way to conduct these types of studies, mostly because the information is already there and requires a person's consent to access it. Moreover, Apple insures that the data shared will be encrypted, will not be sold to third parties and will inform the users of how their data was used in the research. As with any information, the users can withdraw at any time and cease sharing their personal health data, such as permitted under Principle 3, section 4.3.8. of the *PIPEDA*.

Moreover, the database would be inspired by the Global Health Observatory (GHO) in the way it would work. The GHO is a portal to health-related statistics of the Member States of the World Health Organization (WHO), of each of the 194 countries[426]. It is divided by themes such as the global situation and trends which are updated regularly through core indicators. The users of the GHO database are able to select specific indicators such as health topics by country or region and can even download the data in an Excel format. The data extracted includes statistics from every Member State country and allows the WHO to issue analytical reports on key priority health issues, along with annual publications. The purpose of the GHO is to provide an easy access to the data and statistics of the Member States while analyzing and monitoring global and regional

---

[424] Sarah PEREZ, "Apple is launching a Research app that will allow US consumers to participate in health studies", *TECHCRUNCH*, September 10, 2019, online: <https://techcrunch.com/2019/09/10/apple-is-launching-a-research-app-that-will-allow-u-s-consumers-to-participate-in-health-studies/> (accessed on December 10, 2019).

[425] *Id*.

Also see: Sarah PEREZ, "Apple Research app arrives on iPhone and Apple Watch with three opt-in health studies", *TECHCRUNCH*, November 14, 2019, online: <https://techcrunch.com/2019/11/14/apple-research-app-arrives-on-iphone-and-apple-watch-with-three-opt-in-health-studies/> (accessed on December 10, 2019).

[426] WORLD HEALTH ORGANIZATION, "Global Health Observatory (GHO) data", online: <https://www.who.int/gho/about/en/> (consulted on February 17, 2020).

health related issues[427]. To get this data, the WHO uses multiple data providers such as "civil registration authorities, population censuses, household surveys, administration reporting systems, surveillance systems and facility reporting systems of member states"[428]. Such data is compiled on an annual basis and updated into the database while the observatory updates every one or two weeks.

Similarly, all that would be required to generate the national and international database is the consent of the users of smart health technologies and their information would automatically be shared anonymously into the database. Just like the Google queries, what would be generated are statistics and not personally identifiable information. It would become possible to see in what regions certain health problems arose and to track the spread of them through time and space. However, private companies also need to agree to have their users' information shared. Moreover, the sharing of such information needs to be in conformity with the *PIPEDA* and all provincial laws regarding the protection of personal data.

The data would be generated simultaneously by both national and the international databases once the individual consent is given. It would be taken from the second category of smart devices from the three established early on; the ones that could potentially reveal sensitive information on its users, namely smart health devices. However, some authors only distinguish two categories: simple devices with limited capabilities that usually have a very specific purpose such as monitoring a person's physical activity, and advanced devices that perform a variety of tasks such as smart watches with embedded OS, meaning it enables and allows the installation of third-party applications that are available in smartphones[429]. The difference is important because the chances of collecting data from both are different. The first option does not facilitate the transfer of data to a third party, such as it is done in the second option with more advanced technologies. With these devices, there are two types of scenarios in which the users' information is recorded. There are proprietary systems and third-party systems[430]. The first are things such as wearable devices, apps and cloud servers, allowing for the collection of data to

---

[427] HEALTH INFORMATION AND QUALITY AUTHORITY, "WHO Global Health Observatory", online: <https://www.hiqa.ie/areas-we-work/health-information/data-collections/who-global-health-observatory> (consulted on February 17, 2020).
[428] *Id*.
[429] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119.
[430] *Id*., point 3.1.

perform analytics while providing data and results to both the user and other third parties. The second are services, apps, wearables and programs developed by third parties intended for specific functionalities: data collection, data transfer, data storage and data analysis[431]. This means that the users' data is captured by sensors on their devices. It is then collected and transferred to a computer or to a smartphone before being transferred into a permanent data storage. This is done "through proprietary solutions or using third-party apps and programs"[432]. When it is transferred into a permanent data storage, both the users and third parties can have access to this information. Finally, proprietary and third-party servers perform data analysis to provide results to the user. Third parties are able to collect data on wearables and to send it to other systems using SDK's, a collection of software, while proprietary warehouses and cloud services can provide software such as REST API that allows third parties to access the data of users of wearable devices. Although, sometimes third parties need a specific permission to access certain data even if they are granted access through REST API, which is the case mainly for Fitbit. In comparison, the national and international database, after receiving individual consent from the users, would be able to have such information shared and stored within the database. While third parties would be able to cater to individual users, the databases would serve to analyze the data as a whole instead of focusing on individual data.

The transfer to third-party servers is done in two main modes, either by wearable data transfer or by warehouse data transfer[433]. The latter does not collect data in real time and may take several days to transfer the data from the wearable device to the proprietary warehouse, as compared to the first one which transfers raw data. The warehouse data transfer also performs a kind of summarization of the data while the other transfers raw data. In both modes, wearable and warehouse, access to data can either be direct or indirect. The direct transfer is done through the two modes mentioned above allowing a third-party to collect data from the source, whereas the indirect method requires an intermediary system such as a PC or a cellular device before allowing the transfer to occur. The risk with the collection of such data is that users' health can be monetized in order to influence consumer behavior, as explained in the report *Health*

[431] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119, point 3.1.
[432] *Id*., point 3.1.
[433] *Id*., point 3.2.

Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection[434]. What we would be looking for, nonetheless, is the wearable data transfer as the direct transfer would allow analyzing data in real time. Therefore, wearable device vendors such as IOS could provide SDK's that could enable the development of apps for smart wearable devices to directly collect and send out data to third-party servers, in this case to national and international databases[435]. It is to note that for now, only two platforms, mainly Google fit and Microsoft health, offer SDK-Sensors which allow for the collection of data directly from the wearable smart health devices[436]. Moreover, the direct access wearable data transfer between wearables and third-party servers it not yet a viable solution, but is possible[437].

Other solutions include wearable data transfer through an indirect access such as through a smartphone. An app could collect the data and send it to the server, but an app would have to be installed in the wearable and a native app in a smartphone to be able to collect data in real time[438]. However, if the Internet connection is broken, this impedes on data collection and some data such as the heart rate or skin temperature can be lost. Another solution is the warehouse data transfer through direct access. A third-party server could obtain data from wearable smart devices through proprietary warehouse REST API, thus by requesting such data from the wearable warehouse[439]. The fourth solution is the warehouse data transfer though indirect access. This option requires an intermediate smartphone to access the data from the proprietary warehouse. An app from the smartphone then sends the data to a third-party server. This would be a viable solution in case the warehouse does not provide a REST API but allows the operation of an SDK[440]. Amongst all the options listed above, the one that is the most supported by numerous platforms is the warehouse data transfer through a direct access[441].

---

[434] Kathryn C. MONTGOMERY, Jeff CHESTER, and Katharina KOPP, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection*, Washington, Center for Digital Democracy, 2017, on page 14, online: <https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf> (accessed on March 21, 2019).
[435] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119, point 3.2.
[436] *Id*., see Table 1.
[437] *Id*., point 3.2.4.; Miroslav MUZNY et. al., "Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile health monitoring systems", (2020) 133 *Int. J. Med. Inform*., p. 4.
[438] *Id*., point 3.2.1., Link 2.
[439] *Id*., point 3.2.2., Link 5.
[440] *Id*., point 3.2.3., Link 7.
[441] *Id*., point 3.2.5, see Table 2.

This is indeed supported by wearables such as Fitbit, LG Watch R., Microsoft Band and Jawbone UP Move[442]. Fitbit, for example, requires that the user downloads an app to their smartphone or to their computer. The data is then transferred from the wearable to the Fitbit proprietary warehouse. Then, the data becomes available to third parties in the Fitbit proprietary warehouse but because of privacy laws, in order to get such data, Fitbit must consent to share this information with third-party servers. In addition, the LG Watch R. and the Microsoft Band also support wearable data transfer through indirect access; however, not all the data gathered from the available sensors can be collected. Since the data will be stored in a proprietary warehouse, third parties must request permission to access the data[443]. The users of smart health devices would have the option of granting permission to request personal health information to third-parties, in this case the Government and the WHO. When the permission is granted, a token will be provided allowing the third-parties to collect the data from the warehouse. For security reasons, the token would be of limited duration with the option of renewing it[444]. The length of the Fitbit token is of 1 month, the Microsoft Band of 1 hour and the Jawbone UP Move of 1 year[445]. Once such access is granted, it would be possible to get the data on demand through the indirect access or to schedule the collection of data every day, at the same time, once the server updates the tokens.

In any case, the solution chosen must also account for different models of data collection from wearable devices. The recording of data in one wearable could be significantly different from another. As an example, while the Google Fit app is arranged by segments[446] and each segment includes a starting and ending time of a sleep cycle, the Fitbit simply records sleep by minutes[447]. Moreover, wearables do not always collect the same data and distinguish between data names. While Google Fit has four sleep levels "sleep light, deep, REM (Rapid Eye Movement) and awake", Fitbit only has three "sleeping, awake or really awake"[448]. This could potentially make it harder to analyze data generated from different smart health devices as they do not always

[442] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119, point 5.2.1 – 5.2.4.
[443] *Id*., point 5.2.5.
[444] *Id*.
[445] *Id*., point 5.2.5., see Table 5.
[446] A segment happens when a user moves from light sleep to deep sleep as an example; when they do, a new segment is produced. Each segment also includes its own starting and finishing time along with the type of sleep.
[447] *Id*., point 4.1.
[448] *Id*., point 4.2.

compute the same information. If we stay on the example of sleep, temporal discrepancies amongst smart devices are also to account for. Microsoft will mark a sleeping period complete for day 1, if a user slept from day 1 to day 2, but would not compute any sleep for day 1 if the user went to bed past midnight and might compute 2 sleeping periods for day 2. Fitbit only computes one sleeping cycle for the following day and any other sleep periods count as naps[449]. Interoperability amongst the devices must be increased to facilitate data aggregation. As well, we suggest applying advanced analytics to the data retrieved by smart health devices. This has been proven to be successful when large technological companies collaborate together by providing an analytics platform capable of running significant data analytics throughout connected devices[450]. Finally, not all devices have the same counters that compute steps, calories, distance, and more. The Microsoft Band counts them since the last formatting of the device while the Fitbit resets every day[451]. This should be taken into account when comparing the data from different wearable devices.

As for the accessibility of the information to each country, each participating State would only have access to the personal information about the citizens of their own country[452], although the database would allow its Member States to see a general picture of the severity of certain health issues by country or region. The interest of the WHO of having such a database is to track serious health problems and take appropriate measures quickly and effectively to prevent or to reduce the spread of the latter. More specific data would be shared to all Member States if the health issue is a public health emergency of international concern or of interest to international health. This would avoid trade barriers, the prisoner's dilemma and temporal asymmetry in countries with less concerning health problems and would incite more countries to participate in sharing national health information. Nonetheless, for this solution to work, many countries would need to have their own national database able to generate statistics based on the input of smart health devices. The WHO could even send back reports to the participating countries with key health elements to focus on based on the inputs gathered.

---

[449] Francisco de ARRIBA-PÉREZ et. al., "Collection and Processing of Data […]", prev. cited, note 119, point 4.3.
[450] DELOITTE CENTRE FOR HEALTH SOLUTIONS, "Medtech and the Internet of Medical Things | […]", prev. cited, note 188, p. 36.
[451] Francisco de ARRIBA-PÉREZ et. al.,, "Collection and Processing of Data […]", *Ibid*., point 4.4.
[452] While the information will be gathered in an anonymous way, the national database could help pinpoint key health related issues to a certain population or group of people, such as the elderly, of specific ethnical backgrounds, or those living in rural or urban areas, as an example, to determine who are prone to specific health problems.

As well, countries who cannot afford to build a national health database generated by smart health devices can be incited by the WHO to partner up with developed countries in an attempt to work together by providing the resources necessary for data collection and analysis. Similarly to economic partnerships, namely the Canada-United States-Mexico Agreement (CUSMA)[453] where the protection of personal data is covered, there could be partnerships alike where the data of multiple countries is generated in one national database and agreements could cover how the personal data of those involved is protected. Furthermore, some of these agreements could include aid in providing smart health devices to countries where such technologies are less prevalent. This would be a win-win solution for all parties involved[454]. Governments would have access to more information about their citizens and perhaps even those of partnering countries. Individuals would have better assessments of their health and benefit from a quicker and more efficient international response during a health crisis. Private companies who create smart health devices are also progressively turning towards healthcare[455]. They will get access to more information on users and will generate profit by having their technologies sold. In fact, Business Insider Intelligence research has revealed that fitness trackers and other smart health devices in the United States will see a growth of 10% annually and surpass 120 million by the year 2023[456]. With the increase in such technology in the U.S., it would be a matter of time before it spreads worldwide. Therefore, if the access to our personal health data will increase with the use of smart health technologies, the solution would be to put our data to good use so it could benefit us and the world instead of solely benefiting corporate and for profit entities.

---

[453] *Loi portant mise en œuvre de l'Accord entre le Canada, les États-Unis d'Amérique et les États-Unis mexicains*, projet de loi no C-4 (Sanction royale – 13 mars 2020), 1re sess., 43e légis.(Can.), online : <https://www.parl.ca/DocumentViewer/fr/43-1/projet-loi/C-4/premiere-lecture>; OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, "Agreement between the United States of America, the United Mexican States, and Canada", online: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between> (consulted on January 31, 2020). The protection of personal information is covered in section 19.8 in the chapter on digital trade and in section 32.9 in the chapter on exceptions and general provisions. Moreover, section 19.8 (3) lists the principles that are to be followed which consist of "limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability". These principles resemble the ones set out by *PIPEDA*.

[454] Due to the fact that the WHO's legitimacy is currently undermined with the ongoing Covid-19 virus, the institution is underfunded and incapable to offering as much aid to countries as before. Even so, the international organization does not currently have a strong leadership and may not be well equipped to enact our proposed solution and aid its Member States. In such a case, we encourage countries to make bilateral and multilateral agreements to help the less developed countries have access to smart health technologies while ensuring that privacy rights are met through such agreements, just as it can be found in the CUSMA, the new NAFTA agreement.

[455] Kenneth R. FOSTER and John TOROUS, "The Opportunity and Obstacles for Smartwatches and Wearable Sensors", prev. cited, note 183.

[456] Alicia PHANEUF, "Latest trends in medical monitoring devices […]", prev. cited, note 9.

Yet, this data generated by smart health devices should not be used nor analyzed by itself. Just as it is done at the GHO, it would be important to use multiple data sources when analyzing national or global health problems. In sum, the national and international databases would serve as an additional tool to monitor health but it would not be the sole reliable source of information. It would be used in conjunction with what is already done at the GHO along with other WHO health related databases. The reason for it is because such a system will inevitably have flaws. Indeed, considering that the solution of a national database could work in one country, without having the maximum efficiency of internationalizing the database, if the idea of the international database is to be implemented, problems regarding international cooperation are to arise.

Sanctions and Implementation Internationally:

There is a problem of respect of obligations internationally. In order to insure the collaboration of countries in the project of an international database, such a server would have to be placed in the hands of an international entity capable of enforcing international law. In the matter of health, the only international organization with an exclusive mandate for global health is the World Health Organization (WHO). The powers of the WHO are listed in sections 19, 21 and 23 of the *Constitution of the World Health Organization*[457]. As such, the Health Assembly of the WHO can adopt conventions, regulations and make recommendations respectively, as seems fit. We believe the best way to go forward is for the WHO to eventually adopt a convention on smart health devices and the right to privacy but because this process can be very lengthy, it could begin by giving recommendations in regards to helping each other out, using more of such technologies and how to insure that PII stays protected while inciting countries to adopt such practices to increase awareness on a global scale of what is happening in terms of public health. Going for both would also give countries a choice between a convention and a set of recommendations. In fact, our database solution can only work if countries have sufficient privacy laws in place to protect their citizens. Otherwise, citizens' privacy might be undermined.

Nonetheless, the WHO would not have the power to impose sanctions. The international organization could only impose annual reports from its Member States following the adoption of conventions, regulations or recommendations, such as stated in sections 61 to 65 of the WHO's

[457] *Constitution of the World Health Organization*, July 22, 1946, (1948) 14 R.T.N.U. 185 (n° 221), online: <https://apps.who.int/gb/bd/PDF/bd47/EN/constitution-en.pdf>.

Constitution. Nevertheless, the problem is that *soft laws* in comparison to *hard laws* are difficult to enforce, especially when it comes with costs such as changing domestic policies or investing in new technologies. Although *soft laws* are easier to implement, they cannot force States to spend their resources; however, what we can hope for with softer laws is that they create a consensus throughout time amongst the international population and that countries voluntarily agree to abide by the WHO's recommendations if they acknowledge the perceived benefits of them. If they do so, we will achieve international collaboration such as it is mandated under section 44 of the WHO's *International health regulations (2005)*[458]. Indeed, as stated in section 44 (b), Member States must cooperate with each other through "technical cooperation and logistical support"[459] which would complement the idea that State Parties can exchange technologies for skills, information or other needs. The WHO would have to collaborate as well with State parties to provide or facilitate this kind of support[460].

Nonetheless, in order for the international organization to do so, it would require not only global participation of its Member States but also a significant increase in the assessed contributions based on its "wealth and population"[461] to account for the international database and an increased need in cooperation to achieve the solution's desired goal. Presently, the WHO's budget for 2020 to 2021 is set at $4.84 billion[462] but it is composed of assessed contributions which are flexible and voluntary contributions which are given for precise objectives. The latter are generally not flexible and cannot be used for another purpose other than the one for which they were granted. In fact, while decades ago the WHO's budget was composed mainly of assessed contributions, it

---

[458] *International Health Regulations (2005)*, prev. cited, note 289, article 44; Isabelle DUPLESSIS, "Un abrégé de l'histoire des normes de l'OIT et de leur application", in P. VERGE (dir.), *Droit international du travail, Perspectives canadiennes*, Cowansville, Édition Yvon Blais, 2010, 63p, pp. 80-81; 109; Lawrence O. GOSTIN and Allyn L. Taylor O'NEILL, "Global Health Law: A Definition and Grand Challenges", (2008) 1 *Public Health Ethics* 53, on page 57; Brigit TOEBES, "International health law : an emerging field of public international law" (2015) 55 *Indian Journal of International Law* 299, point 3.2.

[459] *International Health Regulations (2005)*, *Ibid*., article 44 (1) (b).

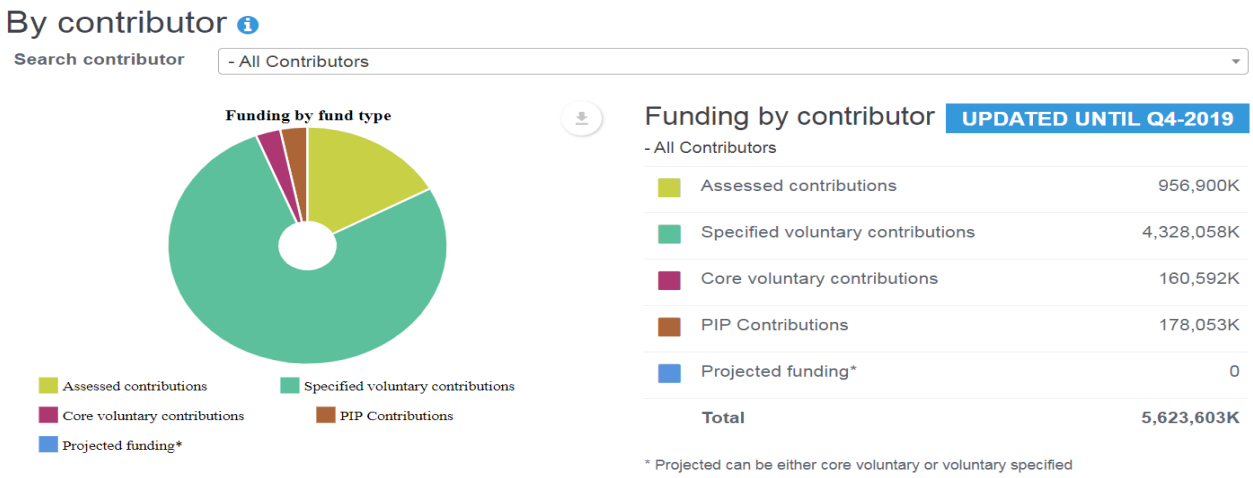
[460] *Id*,, article 44 (2) (b).

[461] WORLD HEALTH ORGANIZATION, "Assessed contributions", online: <https://www.who.int/about/finances-accountability/funding/assessed-contributions/en/> (consulted on April 27, 2020).

[462] WORLD HEALTH ORGANIZATION, *Programme budget 2020-2021*, May 2019, p. 6, online: <https://www.who.int/about/finances-accountability/budget/WHOPB-PRP-19.pdf?ua=1> (consulted on April 27, 2020).

is now mostly comprised of voluntary contributions, as seen in figure 1, which means that the WHO is no longer solely in control of its investments and resource allocation[463].

Figure 1



Source: WORLD HEALTH ORGANIZATION, "Contributors", online: <https://open.who.int/2018-19/contributors/contributor> (consulted on April 27, 2020).

Therefore, in order to implement an international response based on the data generated, the WHO's budget should account for new means of monitoring public health concerns and, if need be, increase the assessed contributions of each Member State.

2. The Population's Advantage in a Database Generated by Smart Health Devices

a) Enhancing Safety, Security, Efficiency and Overall Wellbeing

While considering the global advantages of a database solution that States and the WHO may benefit from, lest we forget the numerous collective advantages of implementing these databases. Nonetheless, while we have demonstrated that the protection of privacy is important and valued in a modern society, it is more so in Western countries as people from other nations such as China are willing to sacrifice their privacy if it means living in a safer and a more secure environment.

Indeed, when it comes to health, most people would not be opposed to their personal information being used for medical purposes, as long as it can eventually prevent or cure a certain health

[463] WORLD HEALTH ORGANIZATION, "A proposal for increasing the assessed contribution", 2016, online: <https://www.who.int/about/finances-accountability/funding/financing-dialogue/assessed-contribution.pdf> (consulted on April 27, 2020).

problem or benefit them directly[464]. The moment a person would begin to object is usually when the information gathered is used in any way against them or to their disadvantage, or worse, to discriminate or incriminate them. Surprisingly, there are societal exceptions. To demonstrate, China's social credit system, which began with regional pilots, is the best and scariest example of a Black Mirror episode come to life. This project aims at crediting, thus giving points to law-abiding citizens; nonetheless, it does so by invading their private lives to the fullest with nearly 200 million CCTV cameras across China aimed at gathering information about what people eat, buy in stores, who their partner is, to who their friends and family are[465]. People with a higher score get access to more and to better things such as hotels, cheaper loans, better universities and better jobs, while people with a lower score could be denied travel, credit or government jobs and can even be locked out of society. Nonetheless, with a growing population of over a billion people, this to them seems like a fair tradeoff and "as a form of social management"[466]. Withal, while this might seem to be a violation of people's privacy and unacceptable in Canada, some users of smart health devices make a similar compromise: privacy for health.

Indeed, people suffering from certain health conditions might find that it is in their interest to risk having their right to privacy violated in exchange of a longer and healthier life with the help of health monitoring devices. As well, we have seen that people can benefit from the use of smart health devices to get a better health insurance rate, for example. While in some areas of China, CCTV cameras are the ones monitoring citizens which are granted rewards or imposed consequences for certain behavior, in other countries such as Canada, our wearables do the same. They can either be used to benefit us when it comes to insurance, if we follow a healthy lifestyle, or be used against us in a work environment. Both scenarios are similar; the difference is in who has access to PII. While China's social credit system monitors and records individual activity that is retraceable to a specific person, the idea behind a national and international database is for

---

[464] Jeroen VAN DEN HOVEN, "Information Technology, Privacy […]", prev. cited, note 73, p. 314.

[465] Matthew CARNEY, "Leave no dark corner", *ABC NEWS*, September 17, 2018, online : <https://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page%3A%20ABC%20Australia-Facebook_Organic&WT.tsrc=Facebook_Organic&fbclid=IwAR1eiJG-W3lCnyM6A1a0htPIatxwjOQDCj9YEUe4GZZ9WODFCJKqbOjIhEg> (accessed on March 19, 2019).
Also see: Padraig MORAN, "How China's 'social credit' system blocked millions of people from travelling", *CBC RADIO*, March 7, 2019, online: <https://www.cbc.ca/radio/thecurrent/the-current-for-march-7-2019-1.5046443/how-china-s-social-credit-system-blocked-millions-of-people-from-travelling-1.5046445> (accessed on August 7, 2020).

[466] Padraig MORAN, "How China's 'social credit' system blocked millions of people from travelling", *Ibid*.

it to keep the data anonymous. The idea is to ensure that the population is protected from health risks instead of using the data against the users of smart technologies. Certainly, we have acknowledged that there are many risks in using these devices for health purposes and increasing the availability of personal health data is amongst the highest. Yet, if these databases can prevent the rate of occurrence and spread of future diseases or even detect early stages of epidemics, it would not only benefit a country's population but also its economy and their overall wellbeing.

The spread of the new coronavirus has put a toll on the global economy and has destroyed the economic growth while leaving many jobless[467]. This virus has affected global shares, stock markets, oil prices and the International Monetary Fund (IMF) even believes that global economy risks a recession and will shrink by 3%[468]. More so, if the recent quarantine due to COVID-19 were to last until August 2020 or later, this would create a massive hit to the Canadian Gross Domestic Product (GDP) which would be worse than during the 2008 and 2009 financial crisis[469]. In addition, during March 16 to March 22, it is estimated that nearly 927,000 Canadians became unemployed[470]. When it comes to privacy concerns and not being able to pay the bills, one might image what the biggest risk truly is. Not to mention that for those who have not lost their jobs during this pandemic and are considered as essential workers such as firefighters, wearing smart health devices can help them during dangerous situations such as falls by connecting to emergency services when needed. This is the case with the Apple Watch Series 4 or later[471]. Yet, this can be useful for anyone feeling ill or lightheaded. If a user of the device falls and stays immobile for a minute, the device will call emergency services automatically by itself. This being said, consumers can greatly benefit from the use of smart technology in relation to their health, but in order to maximize its use and to favor the advantages, these devices can benefit a population if the data generated can be compared and analyzed by health authorities responsible for decision making. On its own, the data can only serve individual purposes, but combined, it can reveal patterns in a community that can help with early-on diagnosis.

---

[467] Lora JONES, Daniele PALUMBO and David BROWN, "Coronavirus: A visual guide to the economic impact", *BBC NEWS*, April 27, 2020, online: <https://www.bbc.com/news/business-51706225> (consulted on April 28, 2020).
[468] *Id*.
[469] Pete EVANS, "How bad will Canada's COVID-19 recession be?", *CBC NEWS*, March 27, 2020, online: <https://www.cbc.ca/news/business/covid-19-recession-economy-analysis-1.5510596> (consulted on April 28, 2020).
[470] *Id*.
[471] APPLE, "Use fall detection with Apple Watch", online: <https://support.apple.com/en-us/HT208944> (consulted on April 28, 2020).

The purpose of the database is therefore to maximize the utility of the already used devices by the general population and ensure that their safety and security needs are met by tracking down health disturbances. The use of wearable devices is rapidly growing worldwide from emerging to developed countries and their popularity is increasing, especially in terms of health monitoring[472]. While the population can benefit from personalized assessments generated by their devices, they can also benefit from the limitation of the spread of certain viruses and in turn, from a more stable and progressive economy. This can be achieved similarly to population health management (PHM). PHM is defined as "the aggregation of patient data across multiple health information technology resources, the analysis of that data into a single, actionable patient record, and the actions through which care providers can improve both clinical and financial outcomes"[473]. Only in our case, the data will not be put into a single patient record, but instead, it would be generated anonymously through multiple smart health devices into a database for evaluation and comparison with other data. More so, the ability to use the data provided by smart devices would be extremely useful to public health practitioners who have expanded the range of data sources and even resort to "electronic health records (EHRs) and social media"[474].

As well, both health practitioners and patients can also benefit from the variety of health apps installed on a user's mobile device, connected to their wearables. Indeed, in 2017, the number of health apps available was estimated to be at around 325,000[475]. The diagnostics generated by these apps can help public health agents detect a spike in unusual health patterns, if the data of multiple users can be combined. Such apps are used more and more in patient care[476]. However, when it comes to sharing their data, users can be reluctant to do so. Yet, over one-third (35%) have reported sharing it with other people such as family members (61%), friends (50%) and their doctor (34%)[477], showing an openness to the idea.

---

[472] PWC, "The Wearable Life 2.0: Connected Living in a Wearable World", March 2016, p. 18, online: <https://www.pwc.com/ee/et/publications/pub/pwc-cis-wearables.pdf> (accessed on July 26, 2020).
[473] CANADIAN MEDICAL ASSOCIATION, "The Future of Technology in Health and Health Care: A Primer", 2018, p. 11, online: <https://www.cma.ca/sites/default/files/pdf/health-advocacy/activity/2018-08-15-future-technology-health-care-e.pdf> (accessed on April 29, 2020); PHILIPS, "What is population health management?", online: <https://www.usa.philips.com/healthcare/medical-specialties/population-health/what-is-population-health-management> (accessed on April 29, 2020).
[474] *Id*., p. 11.
[475] Health applications can serve as "[…] diagnostic aids and as reference tools", *Id*., p. 15.
[476] *Id*., p. 16; Guy PARÉ et. al., *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 53.
[477] *Id*., p. 16.

In addition, for the database solution to work, smart health device users would have to agree to share their information anonymously via their wearables or health app. In fact, in a 2017 survey, it was found that at least 24% of Canadians owned a "smart connected device for health and well-being" and 88% of them owned a "bracelet, wristband or watch"[478]. Other smart health devices used by Canadians include bathroom scales (21%), pedometers (13%) and intelligent clothing (4%)[479]. These devices have proven to benefit individual users as 69% of the users using the devices believed they had maintained or improved their health, 58% felt more confident taking care of their health through the use of these devices and 41% agreed that such devices help them have clearer and more informed conversations with their doctor. Most of the users (85%) were overall satisfied with these devices and said they would continue their use[480]. Therefore, with a decent and growing amount of users of smart health devices, it would be possible to follow, track, monitor and even prevent upcoming diseases if their data were to be available for consultation in one server. The possibility and feasibility of the solution has been confirmed in section *c) Why the Database Solution can Work and Benefit both Users and the General Population*. Yet, for our solution to be fully implemented, it would require a long-term research agreement with the brands that market smart heath devices that would share the data of their users with the databases[481]. However, for the brands to give such consent, they would need the approval of their device users. These users could be reluctant to share more of their data due to the privacy concerns discussed above. We nonetheless believe that the overall benefits generated by smart health devices, mainly health related, which transcend to other fields such as the economy, can outweigh the potential consequences, covered or not by our laws. Moreover, with new updates to the *PIPEDA* based on the Digital Charter along with an increased awareness for privacy rules used in international agreements, we believe that the probability of a breach in privacy does not surpass the benefits of improving individual, national and global health.

---

[478] CANADIAN MEDICAL ASSOCIATION, *The Future of Technology in Health and Health Care: A Primer*, p. 20; Guy PARÉ and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, prev. cited, note 9, p. 38.
[479] *Id*., p. 20.
[480] *Id*., p. 20.
[481] Cecile VIBOUD and Mauricio SANTILLANA, "Fitbit-informed influenza forecasts", (2020) 2 *THE LANCET DIGITAL HEALTH*, online: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30241-9/fulltext> (accessed on May 7, 2020).

Conclusion

In essence, it is safe to say that the global benefits of using personal health data outweigh the consequences of a potential violation of the right to privacy. As a matter of fact, we have seen that there are many laws in Canada protecting personal data which are applicable either to the Government or to private entities. Although there is still an uncertainty regarding the law, the consequences of violating the right to privacy do seem justifiable as they serve a greater good; whether it is to put criminals in jail or to improve overall health, individually and globally. Indeed, in terms of risks on the individual level, we have seen the importance of protecting a user's privacy and how such protection is offered in Canadian legislation.

Moreover, in terms of laws, the jurisprudence regarding section 8 of the *Canadian Charter of Rights and Freedom* should establish a greater legal certainty through laws or uniform jurisprudence to mitigate unlawful intrusion into people's lives. In order to do so, we suggested using Lee-Ann CONROD's three categories of smart devices which would help distinguish what would constitute a violation of section 8 of the *Canadian Charter* while explaining how the searches ought to be conducted in order not to violate users' reasonable expectation of privacy.

Then, we have tackled the risks and the benefits both the users of smart devices and the Government might encounter. On the individual level, we focused on privacy risks through consensual and non consensual accessibility of user data. One of the problems in regards to data gathering, whether by our devices or a third-party, is that our information becomes vulnerable to hacking, especially if kept for longer than necessary periods of time. This was the case with TJX in 2007, Ashley Madison's, Equifax's' and the Uber data breach, to name a few. The access to user data brings up other concerns such as it being shared with other third-parties, increasing overall availability of the information, some of which is used for advertising. There is also a possibility to deduce additional data from smart devices not covered by a mandate which could result in the breaching of articles 7 and 8 of the *Canadian Charter of Rights and Freedom*, therefore violating a person's right to liberty and against unreasonable search and seizure. This said, the infringement of the right to privacy can also lead to an infringement of the right to dignity, another constitutional right. Moreover, we covered the risk of smart devices turning against the users themselves, whether for insurance claims or criminal charges. The problem

with criminal charges in particular, in Canada, is that in contrast to the United States where illegally obtained evidence will defeat the investigation, even considering the administration of justice, in Canada, when evidence is obtained illegally, it will be a question of assessing the impact on the administration of justice. This could mean that information obtained illegally, in violation of a person's reasonable expectation of privacy, could potentially be used in Court, further infringing on users' right to privacy.

Following the latter, we discussed the risks the Government might face if it went through with the solution of building a national database generated by smart health devices. We have seen that the Government ought to be careful in regards to individuals' information as the right to privacy in Canada is highly valued. Therefore, the risk of Canadian's information being seized by foreign jurisdictions or hacked is worrisome. Considering the rise in ransomware such as WannaCry, collecting personal health information of Canadians into one database is quite risky. We have seen that *The State of Healthcare Cybersecurity* report has shown a 60% increase in 2019 of threat detections coming from healthcare organizations. One of the reasons for targeting healthcare specifically is due to their large databases which contain personally identifiable information and give access to other devices connected to the network. The sensitive information accessed by cybercriminals gives them a high return on investment. The data stolen could also be used to commit fraud and identity theft. This is also made easier through smart health devices connected to the Internet of Things (IoT) as having more connected devices would mean they are more likely to get infected and a higher infection rate would make them more susceptible to malware. In addition, we also covered some of the more technical problems that could arise from the solution of creating a database generated by smart devices. The problems included a lack of sample size, lack of participation, the right of an individual to stop sharing personal data at any time, false positives and the connectivity and availability of the devices. While these are just some of the problems, user mistrust of such a solution should also be foreseen as they might not want their personal and sensitive information to be shared with the Government.

Having in mind the potential risks associated with smart health devices used in healthcare and in public health, we covered the advantages both the Government and the users have of using smart health devices and how they can benefit from a database solution. We began by analyzing the Government's advantages which we kept brief, as the point is to benefit users and the community

more than the Government. The latter's benefits should not exceed its population's. Nonetheless, we believe that a national database can benefit the Government by allowing it to a have a vast array of data on its population, cater accordingly its services, allow for more funding in certain designated fields, and make policies which benefit a society as a whole. Additionally, the use of smart devices in healthcare could reduce costs while improving people's overall health. The Public Health Agency of Canada can also use this valuable information to track and prevent upcoming diseases, viruses and outbreaks.

Furthermore, we covered the benefits the population can have if they use smart health devices. As seen in the risk section, smart devices can be used against their owners in insurance claims and criminal charges, but such devices can also help law enforcement solve crimes. Therefore, while a user might give up on some of their privacy, their devices can bring them justice by computing data that can be used to solve a criminal offence or back up a work related injury. As well, we covered how smart health devices can help individuals in need, such as those suffering from certain health conditions such as Parkinson's disease. We have also shown how these devices can help identify flu-like-symptoms and differentiate between them, mainly the new outbreak affecting the whole world: COVID-19. In addition, the future of smart health devices is promising. Apart from making our lives a whole lot easier, they benefit our health by tracking down our progress while being able to track down certain symptoms, even before a medical professional can diagnose them. It is especially important for the elderly or for the people that refrain from seeing the doctor on a regular basis. Moreover, we showcased the feasibility of our solution through what is currently done to monitor diseases such as COVID-19 and a study that was made to see if wearables can predict the flu and the Coronavirus while possibly being able to distinguish between different diseases. The outcome was positive in both scenarios.

While the advantages are promising, in order to fully benefit from them, it is important to mitigate the risks both users of smart health devices and the Government might face. Thus, we began by covering some of the risks smart device users might encounter, starting with legal risks. One of the biggest legal risks individuals might encounter in terms of a breach in privacy is being discriminated against due to their health condition. Therefore, to mitigate or to counter this risk, employers should "take all reasonable measures to accommodate, short of undue hardship,

in order to avoid discrimination"[482]. Employees should also consult the appropriate laws and remedies available such as through the *Canadian Charter* and *Quebec Charter*, the *Canadian Human Rights Act* and the *Civil Code of Quebec*, where applicable. The main takeaway would be that legal remedies are available if such a risk were to occur. We also covered how to mitigate the risk relating to the seizure of smart devices which can violate section 8 of the *Canadian Charter of Rights and Freedom*. Yet, while it is possible to challenge a State intrusion through section 24 (2) of the Charter in order to exclude evidence from Court, a search conducted following a warrant is presumed reasonable even if it invades a person's reasonable expectation of privacy. Moreover, law enforcement authorities might not always need authorization before searching electronic devices. This is why we highlighted the importance of taking into account three considerations mentioned by Justice BINNIE in *R*. v. *A.M*. when analyzing the violation of section 8 which are: "minimal intrusion, [specific] nature and high accuracy rate"[483]. Then, we focused more precisely on consent risks. We covered the risks associated with long to unintelligible clauses covered by the *Civil Code of Quebec* and child consent risks that should be closely monitored by their parents and denounced to the OPC. We further covered the risks associated with keeping information for longer than necessary periods of time along with additional consent risks and how to mitigate them through *PIPEDA*. Yet, apart from external ways to mitigate risks, users should also rely on their own judgment and understand their data before they can protect it. Some solutions would include: investing in newer technology and updated models; reduce the storage of personally identifiable information in the devices and deny unnecessary accesses to applications; refrain from using public Wi-Fi; consulting the privacy policy of applications and wearables; limiting the amount of smart devices and devices that are "smart"; and shutting off smart devices that are not in use. These are just a few examples to demonstrate that it is possible to mitigate risks and it is also an individual responsibility.

As for the Government, we focused on the potential hacking risk of personal health information and on the necessity of having uniformity in Canadian health law. In terms of consent, the Government should mitigate this risk by enforcing consent where appropriate and making sure that Canadians' personal health information is not transferred without proper protection such as

[482] Laura BARNETT, Julia NICOL & Julian WALKER, "Background Paper: An Examination of the Duty to Accommodate in the Canadian Human Rights Context,", prev. cited, note 306, at 2.3.
[483] *R.* v. *A.M.,* [2008] 1 SCR 569, 2008 SCC 19 (CanLII), para 13; 42.

required in Principle 4.1.3 of the *PIPEDA*. In terms of the gaps in provincial privacy laws deemed substantially similar to *PIPEDA*, it would be important to have uniformity in the law amongst all Canadian provinces to avoid gaps within it. Moreover, to cope with some of the risks associated with the use of technology, Minister of Innovation, Science and Economic Development Navdeep BAINS announced the creation of Canada's new Digital Charter aimed to modernize *PIPEDA*. Government policies and legislation will be measured against these principles which will increase the control Canadians have over their personal information.

Furthermore, once the risks are mitigated, it then becomes possible to favor the advantages. The Government can favor the advantages of having smart devices in healthcare by creating a national database which would work in conjunction with an international database at the WHO. The national advantages would indeed increase if an international organization capable of monitoring global health could use live data generated from an objective source to predict and implement timely measures towards stopping the spread of an infectious disease. Since partnerships between the WHO and private parties have previously been made, the feasibility of this idea is not challenged but would require further cooperation between private entities and users of these devices. Such a solution would also benefit the WHO as it has been criticized for its slow reactions to epidemics and capacity to adapt to a fast changing environment. Even so, apart from improving disease monitoring, the WHO could enhance its data on the overall health rate of populations around the world and address its other main issues such as obesity.

The population, on the other hand, can favor the advantages by increasing their use of smart health devices and allowing the data to be extracted into the database. If their data can be monitored by public health authorities and by the WHO, it would enhance their safety, security, efficiency of healthcare and their overall wellbeing. We have also seen that some people from China would not be opposed to giving up their privacy if it meant increasing their security, such as demonstrated in China's social credit system. The same could be said about people suffering from grave health conditions who could benefit from smart health devices and a quicker and improved patient-doctor care. Nonetheless, as we have seen, outbreaks have severe repercussions on people and on the economy. Thus, the benefits of using smart health devices are not only seen in healthcare but also in other sectors, impacting a population's overall wellbeing. Therefore, to increase these advantages, the data generated should be compared and analyzed by health

authorities responsible for decision making. As said, the purpose of the database is therefore to maximize the utility of the already used devices by the general population and ensure that their safety and security needs are met by tracking down health disturbances. In any case, for the solution to work, it would require a long-term research agreement with the brands that market smart heath devices that would share the data of their users with the database, and for that, users would need to give their consent and trust that their personal data is well protected.

Continued Discussion

Admissibility of Proof in Courts

There are also consequences in terms of the admissibility of proof in courts as any potential data can only be admissible in Court if not tempered with[484]. Although recordings are admissible in Court, the tempering of them is not. There are also different legal requirements to fulfill before a piece of evidence is admissible in Court depending in which category of evidence the device falls into[485]. As it was said in *Benisty* c. *Kloda*, an audio recording may be described as a "material element" of proof, covered by article 2855 of the *Civil Code of Quebec* (C.c.Q.), or as a “testimony” as seen in article 2874 of the C.c.Q., depending on the intended utility of the document[486] and the temporality that it falls into. As seen in *Benisty* c. *Kloda*, in the case of a recording, for example, the party that uses it as proof must firstly prove its authenticity in regards to articles 2855 and 2874 of the C.c.Q. However, they will not have to prove the reliability of the technological support because of the presumption in its favor established by article 7 of the *Act to establish a legal framework for information technology*[487]. It was further said that the recordings must also be sufficiently intelligible, audible and understandable[488]. If health data were to be presented in Court, provided by smart devices, would it fill these criteria? The fact that personal data is most likely subjected to being transferred rather than copied implies new legal concerns, mostly the obligation of documenting the whole process in order to insure the

---

[484] *Benisty* c. *Kloda,* prev. cited, note 359, para. 26.
[485] Vincent GAUTRAIS and Patrick GINGRAS, “La preuve des documents technologiques”, (2010) 22 *Les Cahiers de propriété intellectuelle* 267, online : <https://cpi.openum.ca/files/sites/66/La-preuve-des-documents-technologiques.pdf>.
[486] *Benisty* c. *Kloda, Ibid*., para. 118.
[487] *Loi concernant le cadre juridique des technologies de l'information*, prev. cited, note 52.
Also see: *Benisty* c. *Kloda, Ibid*., para. 112.
[488] *Benisty* c. *Kloda*, *Ibid*., para. 124.

integrity of the data provided[489]. Essentially, the data gathered and analyzed would have to match the data provided to the Court; thus, the data has to be authentic[490]. However, in the scenario that personal health data generated by smart devices could be admissible in Court, we would not want to create a precedent in which courts and law enforcement officers "look over our physician's shoulder" in order to access our data because that would infringe on our right to a "reasonable expectation of privacy"[491] regarding our health data. Yet, it is intriguing to consider what our right to privacy holds with smart devices on the rise. How courts will use them going forward is, for now, only up to our interpretation.

Once smart health devices are permitted in Court, certain disclosures concerning the privacy of the users would be lawful in the circumstances where they constitute matters over which the public would have a legitimate interest in being informed, such as was noted by KAYSER[492]. Public interest is therefore an essential consideration in regards to privacy rights[493]. This is where the reasonable expectation of privacy established by courts comes into play based on different situations a person can be in, such as within a private area or in a public space. The latter might not enable a person to a reasonable expectation of privacy, but as we have seen, privacy is not an "all-or-nothing concept"[494]. Nonetheless, while violations of section 8 of the *Canadian Charter* might still persist due to the inconsistency of Canadian case law, we have seen that a search conducted following a warrant is presumed reasonable even if it invades a person's reasonable expectation of privacy, regardless of circumstances differentiating between private and public spaces. Thus, once the data is accessed from smart health devices, there is no avoiding an intrusion of the user's right to privacy, unless the user deliberately consents to giving away their

---

[489] *Benisty* c. *Kloda,* prev. cited, note 359, para. 135-137.
Also see: *Loi concernant le cadre juridique des technologies de l'information*, prev. cited, note 52, articles 17 et 18.
[490] *Benisty* c. *Kloda, Ibid*., para. 138.
[491] Dylan ROSKAMS-EDRIS, "The Eye Inside: Remote Biosensing Technologies in Healthcare and the Law", prev. cited, note 98, p. 74.
[492] Pierre TRUDEL and Karim BENYEKHLEF, "Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes", p. 8, online : <https://depot.erudit.org/bitstream/002690dd/1/0072.pdf> (consulted on May 18, 2020).
Also see : Pierre KAYSER, *La protection de la vie privée par le droit. Protection du secret de la vie privée*, 3e éd., Paris, Economica, 1995, n° 135, p. 235.
[493] *Valiquette* c. *The Gazette*, [1991] R.J.Q. 1075.
[494] Pierre TRUDEL and Karim BENYEKHLEF, "Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes", *Ibid*., p. 9.
Also see : *R*. v. *Jarvis*, prev. cited, note 201.
Also see : K. BENYEKHLEF, E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", prev. cited, note 34, para. 70.

right, which would not be the case if a warrant is needed to access such data. Then again, if a mandate were to cover specific sought out information, nothing would stop law enforcement from getting access to other incriminating pieces of data that could still be used in Court considering the administration of justice.

This said, smart health devices raise a few concerns whether in terms of being admissible to Court or insuring that privacy rights of their user are not breached in the process. We therefore insist on opening up a discussion in this matter to further analyze how our laws can protect personal information from unjust intrusion, namely by law enforcement. If smart health devices are to be used in healthcare and in public health to the detriment of user privacy rights, greater protections should be established to avoid legal uncertainty and user mistrust. We also wonder what would happen if foreign governments got a hold of such information. How would the power dynamic between countries then be affected?

In essence, we have seen that our personal information could be subpoenaed by a Court or used in an investigation; hence, it becomes important not only to keep our personal data within our own borders, to the extent to which it is possible, but also to set a clear jurisprudence to ensure the respect of sections 7 and 8 of the *Canadian Charter*. In this regard, a solution we have established to benefit from smart health devices is to create a national and an international database at the WHO capable of generating inputs from smart health devices and tracking down the progression of health issues. As we were able to see, while there are individual benefits to using such devices, when applied to a global scale, they offer insights into health like never seen before by being able to track previously unreported cases, along with their spread and their progression. Essentially, smart health devices do offer additional health benefits for their users and the community, but the system might abuse their rights by abusing surveillance. Synchronization and uniformity is therefore needed amongst the laws in place, the jurisprudence and what is done in practice based on the evolution of technology and our moral values. After all, we cannot enhance a protection by limiting another; a balance should be established between "privacy rights, economic interests, security and other important goals"[495].

[495] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy", prev. cited, note 156.

Table of Legislation

Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR, c. A-2.1

Act respecting health services and social services, CQLR, c. S-4.2

Act respecting the protection of personal information in the private sector, CQLR, c. P-39.1

Act respecting the Régie de l'assurance maladie du Québec, CQLR, c. R-5

African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, online: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

American Declaration of the Rights and Duties of Man, April 30, 1948, online: <https://www.cidh.oas.org/Basicos/English/Basic2.American%20Declaration.htm>

Bill 73, *Freedom of Information and Protection of Privacy Amendment Act*, 5th Sess., 37th ParI., 2004

Canada Health Act, R.S.C. 1985, c. C-6

Canadian Human Rights Act, R.S.C. 1985, c. H-6

Charte canadienne des droits et libertés, partie 1 de la Loi constitutionnelle de 1982, [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)]

Charte des droits et libertés de la personne, RLRQ, c. C-12

Charte des Nations Unies, 26 juin 1945, 15 C.N.U.O.I. 365 (entrée en vigueur le 24 octobre 1945)

Charter of Fundamental Rights of the European Union, October 26, 2012, Official Journal of the European Union, 2012/C 326/02, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT>

Constitution of the World Health Organization, July 22, 1946, (1948) 14 R.T.N.U. 185 (n^{o} 221), online: <https://apps.who.int/gb/bd/PDF/bd47/EN/constitution-en.pdf>

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981, S.T.E. n^{o} 108 (entry into force on October 1, 1985)

Convention on the Rights of the Child, November 20, 1989, (1990) 1577 R.T.N.U. 3 (n^{o} 27531) online: <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx> (accession of Canada in 1991)

Criminal Code, R.S.C. 1985, c. C-46

Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies, Rés. AG 2625(XXV), Doc. Off. AG NU, 25e sess., suppl. no 85, Doc. NU A/8082 (1970)

EC, Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1 [GDPR]

Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165

Genetic Non-Discrimination Act, S.C. 2017, c. 3

Guidelines for the Regulation of Computerized Personal Data Files, Rés. 45/95, Doc. off. A.G., (1990), online: <https://www.refworld.org/docid/3ddcafaac.html>

Health Information Act, RSPEI 1988, c. H-1.41

Health Information Act, S.A. 2018, c. H-5

Health Insurance Act, CQLR, c. A-29

International Covenant on Civil and Political Rights, 16 December 1966, 999 U.N.T.S. 171 (came into force in Canada on 19 May 1976 and ratified by Québec on 1 November 1978)

International Covenant on Economic, Social and Cultural Rights, 16 December 1966, 993 U.N.T.S. 3 (came into force in Canada on 19 August 1976 and ratified by Québec on 21 April 1976)

International Health Regulations (2005), May 23, 2005, (2007) 2509 R.T.N.U. 79 (n° 44861), online: <https://apps.who.int/gb/bd/PDF/bd47/EN/constitution-en.pdf>

In the matter of the: Reference of the Government of Quebec concerning the constitutionality of the Genetic Non-Discrimination Act enacted by Sections 1 to 7 of the Act to prohibit and prevent genetic discrimination, 2018 QCCA 2193 (CanLII)

Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1

Loi constitutionnelle de 1867, 30 & 31 Vict., c. 3 (R.-U.)

Loi constitutionnelle de 1982, annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.)

Loi portant mise en œuvre de l'Accord entre le Canada, les États-Unis d'Amérique et les États-Unis mexicains, projet de loi no C-4 (Sanction royale – 13 mars 2020), 1re sess., 43e légis.(Can.)

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, Projet de loi no 64, 1ière session, 42e légis. (Can.)., online : <http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html> (accessed on July 23, 2020)

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5

Loi sur la Santé publique, RLRQ, c. S-2.2

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1

Personal Health Information Act, SNL 2008, c. P-7.01

Personal Health Information Act, SNS 2010, c. 41

Personal Health Information Privacy and Access Act, SNB 2009, c. P-7.05

Personal Health Information Protection Act, 2004, SO 2004, c. 3, Sch A

Personal Information International Disclosure Protection Act, SNS 2006, c. 3

Personal Information Protection Act, S.A. 2003, c. P-6.5

Personal Information Protection Act, S.B.C. 2003, c. 63

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5

Privacy Act, R.S.C. 1985, c. P-21

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, October 10, 2018, S.T.E. no 223

The Madrid Resolution, The International Conference of Data Protection and Privacy Commissioners, November 5, 2009, online: <https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/international_standards_madrid_2009.pdf>

The Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, February 16, 2010, online: <https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf>

Universal Declaration of Human Rights, res. 217A (Ill), Off. doc., U.N.G.A., 3rd Sess., Supp. No. 13 at 71, U.N. Doc. A/810 (10 December 1948)

Table of Judgments

M. (A.) v. *Ryan*, [1997] 1 SCR 157, 1997 CanLII 403 (SCC)

Nammo v. *TransUnion of Canada*, [2010] F.C. 1284 (CanLII)

R. c. *Kang-Brown*, [2008] 1 SCR 456, 2008 SCC 18 (CanLII)

R. v. *A.M.*, [2008] 1 SCR 569, 2008 SCC 19 (CanLII)

R. v. *Cole*, [2012] 3 SCR 34, 2012 SCC 53 (CanLII)

R. v. *Cook*, 1997 CanLII 392 (SCC), [1997] 1 SCR 1113

R. v. *Edwards*, [1996] 1 SCR 128, 1996 CanLII 255 (SCC)

R. v. *Fearon*, [2014] 3 SCR 621, 2014 SCC 77 (CanLII)

R. v. *Gomboc*, [2010] 3 SCR 211, 2010 SCC 55 (CanLII)

R. v. *Hape*, 2007 SCC 26 (CanLII), [2007] 2 SCR 292

R. v. *Jarvis*, 2019 SCC 10 (CanLII)

R. v. *Jones*, [2017] 2 SCR 696, 2017 SCC 60 (CanLII)

R. v. *Marakah*, [2017] 2 SCR 608, 2017 SCC 59 (CanLII)

R. v. *Morelli*, [2010] 1 SCR 253, 2010 SCC 8 (CanLII)

R. v. *Plant*, [1993] 3 SCR 281, 1993 CanLII 70 (SCC)

R. v. *Tessling*, [2004] 3 SCR 432, 2004 SCC 67 (CanLII)

R. v. *Vu*, [2013] 3 SCR 657, 2013 SCC 60 (CanLII)

R. v. *Wise*, [1992] 1 SCR 527, 1992 CanLII 125 (SCC)

Reid v. *Covert,* 354 U.S. 1, 77 S. Ct. 1222, 1 L. Ed. 2d 1148, 1957 US LEXIS 729 (US June 10, 1957)

Syndicat des Enseignant(e)s de Charlevoix v. *CS de Charlevoix*, 2014 CanLII 50053 (QC SAT)

Syndicat canadien de la fonction publique (FTQ, section locale 3535) c. *Société des alcools du Québec (Logistique & distribution)*, 2011 CanLII 84831 (QC SAT)

U. S. v. *Toscanino*, 500 F.2d 267 (2d Cir. 1974)

Valiquette c. *The Gazette*, [1991] R.J.Q. 1075

Bibliography

DOCTRINE

ANDRESS, J., and Mark LEARY, "Protect the Data – Chapter 6", in *Building a Practical Information Security Program*, Syngress, 2015, pp. 103-123, <https://www.sciencedirect.com/topics/computer-science/network-segmentation>

ARRIBA-PÉREZ, F. D., Manuel CAEIRO-RODRIGUEZ and Juan M. SANTOS-GAGO, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", (2016) 16 *Sensors (Basel)* 1538, online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/>

BALDWIN, M. L., & Steven C MARCUS, "Perceived and Measured Stigma Among Workers with Serious Mental Illness", (2006) 75:3 *Psychiatric Services* 388

BARNETT, L., "Canada's Approach to the Treaty-Making Process", (2008) *Library of Parliament* online: <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/200845E>

BARNETT, L., Julia NICOL & Julian WALKER, "Background Paper: An Examination of the Duty to Accommodate in the Canadian Human Rights Context", (2012) *Library of Parliament*, online: <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201201E>

BENYEKHLEF, K., E. PAQUETTE-BÉLANGER and A. PORCIN, "Vie privée et surveillance ambiante : le droit canadien en chantier", (2013) 65 *Droit et cultures* 191, online: <https://journals.openedition.org/droitcultures/3092#ftn115> (accessed on May 23, 2020)

BENYEKHLEF, K., *Une possible histoire de la norme. Les normativités émergentes de la mondialisation*, (2e éd.), Montréal, Éditions Thémis, 2015

BLOOM, A., *The Republic of Plato: Second Edition*, United States, Basic Books, 1991, 512 pages

BOTHA, H., "Human dignity in comparative perspective", (2009) 20 *Stellenbosch L. Rev*. 171

BRAILLARD, P., *Théories des relations internationales*, Paris, Presses universitaires de France, 1977, 459 p

BRIMBLECOMBE, F., and Gavin PHILLIPSON, "Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression", (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 1

BRUNELLE, C., "La dignité dans la Charte des droits et libertés de la personne : de l'ubiquité à l'ambiguïté d'une notion fondamentale", (2006) 66.5 *R. du B*. 143

CAIVANO, N., "Inaccessible Inclusion: Privacy, Disclosure and Accommodation of Mental Illness in the Workplace", (2016) 5-1 *Canadian Journal of Human Rights* 97, 2016 CanLIIDocs 69, <http://www.canlii.org/t/6x1> (retrieved on 2020-03-23)

CENTERS FOR DISEASE CONTROL AND PREVENTION, "Principles of Epidemiology in Public Health Practice, Third Edition: An Introduction to Applied Epidemiology and Biostatistics", *Section 11: Epidemic Disease Occurrence*, online: <https://www.cdc.gov/csels/dsepd/ss1978/lesson1/section11.html> (consulted on January 9, 2020)

CHRISTAKI, E., "New technologies in predicting, preventing and controlling emerging infectious diseases", (2015) 6 *Virulence* 558, online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4720248/>

CLEMENT, A., and Jonathan A. OBAR, "Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers", (2016) 6 *Journal of Information Policy* 294

CONROD, L. A., "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information", (2019) 24 *Appeal: Review of Current Law and Law Reform* 115, online: <http://www.canlii.org/t/sfd8> (accessed on October 28, 2019)

CORRIGAN, P., & Robert LUNDIN, *Don't Call Me Nuts: Coping with the Stigma of Mental Illness*, Illinois, Recovery Press, 2001

D'ASPREMONT, J., "Herbert Hart in today's international legal scholarship", in *International Legal Positivism in a Post-Modern World*, Cambridge, Jörg Kammerhofer, (2014) *Cambridge University Press* 114, online: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/288062FF78419EDDAD235E1E9F2E237C/9781139094245c5_p114-150_CBO.pdf/herbert_hart_in_todays_international_legal_scholarship.pdf >

DE FAUW, J., et. al., "Clinically applicable deep learning for diagnosis and referral in retinal disease", (2018) 24 *Nature Medicine* 1342

DEVLIN, R.F., "Mapping Legal Theory", (1994) 32 *Alta L. Rev*. 602

DUPLESSIS, I., "Un abrégé de l'histoire des normes de l'OIT et de leur application", in P. VERGE (dir.), *Droit international du travail, Perspectives canadiennes*, Cowansville, Édition Yvon Blais, 2010, 63p

DWORKIN, R., *Law`s Empire*, Cambridge, London, Harvard University Press, 1986, 484 p., online: <http://www.filosoficas.unam.mx/~cruzparc/empire.pdf>

FOSTER, K. R., and John TOROUS, "The Opportunity and Obstacles for Smartwatches and Wearable Sensors", (2019) 10 *IEEE* Pulse 22, online: <https://ieeexplore.ieee.org/abstract/document/8666099>

GAUTRAIS, V., "The Colour of E-Consent", (2004) 1 *UOLTJ* 189-212

GAUTRAIS, V., and Patrick GINGRAS, "La preuve des documents technologiques", (2010) 22 *Les Cahiers de propriété intellectuelle* 267, online : <https://cpi.openum.ca/files/sites/66/La-preuve-des-documents-technologiques.pdf>

GEIST, M., & Milana HOMSI, "Outsourcing Our Privacy: Privacy and Security in a Borderless Commercial World", (2005) 54 *U.N.B.L.J*. 272

GOODMAN, M., "Human Dignity in Supreme Court Constitutional Jurisprudence", (2006) 84 *Nebraska Law Review* 741

GOSTIN, L, O. and Allyn L. Taylor O'NEILL, "Global Health Law: A Definition and Grand Challenges", (2008) 1 *Public Health Ethics* 53

GRATTON, E., *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, Toronto, CCH Canadian, 2003

HALLIDAY, J., et. al., "Bringing together emerging and endemic zoonoses surveillance: shared challenges and a common solution", (2012) 367 *Philos Trans R Soc Lond B Biol Sci*. 2872, online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3427560/>

HART, H. L. A., "Positivism and the Separation of Law and Morals", (1958) 71 *Harvard Law Review 593*, online: <http://users.umiacs.umd.edu/~horty/courses/readings/hart-1958-positivism-separation.pdf>

HERT, P. D., and Vagelis PAPAKONSTANTINOU, "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition", (2014) 30 *Computer Law & Security Review* 633, online: <http://www.ejtn.eu/PageFiles/17861/The%20Council%20of%20Europe%20Data%20Protection%20Convention.pdf>

HORMOZI, A. M., "Cookies and Privacy", (2005) 13 *Information Systems Security* 51

KANG, M., Eunkyoung PARK, Baek Hwan CHO and Kyu-Sung LEE, "Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices", (2018) 22 *Int Neurourol J*., online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6077937/>

KARDASH, A., and Patricia KOSSEIM, "Canada", in *The International Comparative Legal Guide to: Data Protection 2018*, London, Global Legal Group, 2018

KAYSER, P., *La protection de la vie privée par le droit. Protection du secret de la vie privée*, 3e éd., Paris, Economica, 1995, n° 135

KELSEN, H., *General Theory of Law and State*, 1st ed., New York, Routledge, 2005, online: <https://doi.org/10.4324/9780203790960>

KOVATCHEV, B. P., et al, "Feasibility of outpatient fully integrated closed-loop control", (2013) 36 *Diabetes Care* 1851

LAFERRIÈRE, C., *États-Unis d'Amérique/Canada : Traité de droit de la sécurité nationale*, Montréal, Wilson & Lafleur ltée, 2018, 1081 pages

LAXMINARAYAN, R., et. al., "Antibiotic resistance—the need for global solutions", (2013) 13 *Lancet Infectious Diseases* 1057

MITCHELL, P., and Jennifer TAYLOR, "Case Commentary on Laushway v Messervey, 2014 NSCA 7; 'Old Evidence Law Dogs, New Technology Tricks", (2015) 12 *Digital Evidence & Elec. Signature L Rev* 13

MONTGOMERY, K. C., Jeff CHESTER, and Katharina KOPP, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection*, Washington, Center for Digital Democracy, 2017

MORAND, C. A., *Le droit néo-moderne des politiques publiques*, Paris, L.G.D.J., 1999

MOTTI, V. G., and Kelly CAINE, "Users' Privacy Concerns About Wearables", in *Financial Cryptography and Data Security*, Berlin, Springer, 2015, online: <https://link.springer.com/chapter/10.1007/978-3-662-48051-9_17>

MUKHOPADHYAY, U., Anthony SKJELLUM, Oluwakemi HAMBOLU, Jon OAKLEY, Lu YU, and Richard BROOKS, "A brief survey of Cryptocurrency systems", (2016) *14th Annual Conference on Privacy, Security and Trust (PST)* 745

MUZNY, M., Andre HENRIKSEN, Alain GIORDANENGO, Jan MUZIK, Astrid GROTTLAND, Håvard BLIXGARD, Gunnar HARTVIGSEN and Eirik ÅRSAND, "Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile

health monitoring systems", (2020) 133 *Int. J. Med. Inform*, online: <https://www.sciencedirect.com/science/article/pii/S138650561831150X>

MYKHALOVSKIY, E., and Lorna WEIR, "The Global Public Health Intelligence Network and Early Warning Outbreak Detection: A Canadian Contribution to Global Public Health", (2016) 97 *Canadian Journal of Public Health* 42, online: <https://www.ncbi.nlm.nih.gov/pubmed/16512327>

NOWELL-SMITH, H., and Hugh O'REILLY, "A Triumph of Substance Over Form in How Discrimination Law Treats Obesity", (2003) 82-3 *Canadian Bar Review* 681, online: <http://www.canlii.org/t/2cjq> (consulted on October 28, 2019)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA and OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA, *Report of an Investigation into the Security, Collection and Retention of Personal Information*, September 25, 2007, CanLII 41283 (PPC), online: <http://canlii.ca/t/1t3tb>

PARÉ, G. and Claire BOURGET, *Diffusion of Smart Devices for Health in Canada*, Montreal, CEFFRIO, 2017, online: <https://www.benefitscanada.com/wp-content/uploads/2017/09/CanadaHealthInfoway_DiffusionofSmartDevicesforHealthinCanada.pdf> (accessed on May 26, 2020)

PENNEY, J., "Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31 *Berkeley Technology Law Journal* 117

RADIN, J. M., Nathan E. WINEINGER, Prof Eric J. TOPOL and Steven R. STEINHUBL, "Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study", (2020) 2 *THE LANCET DIGITAL HEALTH*, online: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30222-5/fulltext> (accessed on May 1, 2020)

Report of an Investigation into the Security, Collection and Retention of Personal Information, 2007 CanLII 41283 (PPC)

ROSKAMS-EDRIS, D., "The Eye Inside: Remote Biosensing Technologies in Healthcare and the Law", (2018) 27 *Dalhousie Journal of Legal Studies* 59

SANTILLANA, M., André T. NGUYEN, Mark DREDZE, Michael J. PAUL, Elaine O. NSOESIE, John S. BROWNSTEIN, "Combining Search, Social Media, and Traditional Data Sources to Improve Influenza Surveillance", (2015) *PLoS Comput Biol*., online: <https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1004513>

SCOTT, C., "Our Digital Selves: Privacy Issues in Online Behavioural Advertising", (2012) 17 *Appeal: Review of Current Law and Law Reform* 63

SOLOVE, D. J., "Conceptualizing Privacy" (2002) 90 *Cal. L. R*. 1087

TOEBES, B., "International health law: an emerging field of public international law" (2015) 55 *Indian Journal of International Law* 299

TRUDEL, P., *Le droit de l'information : une introduction*, Montreal, 17 pages, online : <https://pierretrudel.openum.ca/files/sites/6/2017/07/DroitdelinformationINTRO.pdf> (accessed on October 24, 2019)

TRUDEL, P. and Karim BENYEKHLEF, "Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes", online: <https://depot.erudit.org/bitstream/002690dd/1/0072.pdf> (consulted on May 18, 2020)

ULLA, M., "L'obésité d'un travailleur constitutive d'un handicap relevant de la protection de la Directive 2000/78 – L'évolution récente de la notion de handicap en droit de l'Union européenne", (2015) 28-1 *Revue québécoise de droit international* 185, online : <http://www.canlii.org/t/2sbv> (accessed on October 8, 2019)

Use of sensitive health information for targeting of Google ads raises privacy concerns, 2014 CanLII 3357 (PCC), online: <http://canlii.ca/t/g2wqw>

VAN DEN HOVEN, J., "Information Technology, Privacy, and the Protection of Personal Data", (2008) *Information Technology and Moral Philosophy* 301

VERMA, M., Kamal KISHORE, Mukesh KUMAR, Aparajita RAVI SONDH, Gaurav AGGARWAL, Soundappan KATHIRVEL, "Google Search Trends Predicting Disease Outbreaks: An Analysis from India", (2018) 24 *Healthc Inform Res* 300

VERMA, M., Kamal KISHORE, Mukesh KUMAR, Aparajita RAVI SONDH, Gaurav AGGARWAL, Soundappan KATHIRVEL, "Google Search Trends Predicting Disease Outbreaks: An Analysis from India", (2018) 24 *Healthc Inform Res* 300

VIBOUD, C., and Mauricio SANTILLANA, "Fitbit-informed influenza forecasts", (2020) 2 *THE LANCET DIGITAL HEALTH*, online: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30241-9/fulltext> (accessed on May 7, 2020)

XIA, F., Laurence T. YANG, Lizhe WANG and Alexey VINEL, "Internet of Things", (2012) 25 *Int. J. Commun. Syst*. 1101

YANG, S., Mauricio SANTILLANA, and S. C. KOU, "Accurate estimation of influenza epidemics using Google search data via ARGO", (2015) 112 *Proc Natl Acad Sci USA*, online: <https://www.pnas.org/content/112/47/14473> (consulted on May 7, 2020)

YIN, Y., Yan ZENG, Xing CHEN, and Yuanjie FAN, "The internet of things in healthcare: An overview", (2016) 1 *J Ind Inf Integr* 3, online: <https://www.sciencedirect.com/science/article/pii/S2452414X16000066>

ZANINOTTO, P., George David BATTY, Sari STENHOLM, Ichiro KAWACHI, Martin HYDE, Marcel GOLDBERG, Hugo WESTERLUND, Jussi VAHTERA and Jenny HEAD, "Socioeconomic Inequalities in Disability-free Life Expectancy in Older People from England and the United States: A Cross-national Population-Based Study", (2020) XX *Journals of Gerontology: Medical Sciences*, online: <https://academic.oup.com/biomedgerontology/advance-article/doi/10.1093/gerona/glz266/5698372>

INTERNET SOURCES

ABRAMS, R., "Target to Pay $18.5 Million to 47 States in Security Breach Settlement", *THE NEW YORK TIMES*, May 23, 2017, online: <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html> (accessed on October 4, 2019)

AGENCE FRANCE-PRESSE, "Ebola : la réaction rapide de l'OMS saluée, mais bémol sur la prévention", *RADIO-CANADA*, May 25, 2018, online : <https://ici.radio-canada.ca/nouvelle/1103282/ebola-reaction-rapide-oms-saluee-prevention-critiquee-organisation-mondiale-sante-virus-vaccin> (accessed on October 28, 2019)

AHMAD, T., "Online Privacy Law: Canada", *LIBRARY OF CONGRESS*, June 2012, online: <https://www.loc.gov/law/help/online-privacy-law/2012/canada.php> (consulted on March 26, 2020)

ALJAZEERA, "Coronavirus: All you need to know about symptoms and risks", February 11, 2020, online: <https://www.aljazeera.com/news/2020/01/coronavirus-symptoms-vaccines-risks-200122194509687.html> (consulted on February 11, 2020)

APPLE DEVELOPER, "Monitoring Movement Disorders", online: <https://developer.apple.com/documentation/coremotion/monitoring_movement_disorders> (consulted on October 25, 2019)

APPLE NEWSROOM, "Stanford Medicine announces results of unprecedented Apple Heart Study", March 16, 2019, online: <https://www.apple.com/newsroom/2019/03/stanford-medicine-announces-results-of-unprecedented-apple-heart-study/> (consulted on December 10, 2019)

APPLE NEWSROOM, "Apple announces effortless solution bringing health records to iPhone", January 24, 2018, online: <https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/> (consulted on October 25, 2019)

APPLE NEWSROOM, "Apple opens Health Records API to developers", June 4, 2018, online: <https://www.apple.com/newsroom/2018/06/apple-opens-health-records-api-to-developers/> (consulted on October 25, 2019)

APPLE, "Use fall detection with Apple Watch", online: <https://support.apple.com/en-us/HT208944> (consulted on April 28, 2020)

BBC, "Fitbit contradicts husband's story of wife's murder – police", April 27, 2017, online: <https://www.bbc.com/news/world-us-canada-39710528> (consulted on October 24, 2019)

BBC, "Fitbit data used to charge US man with murder", October 4, 2018, online: <https://www.bbc.com/news/technology-45745366> (consulted on October 24, 2019)

BEACON LAW CENTER, "New Data Breach Reporting Rules", March 29, 2019, online: <https://beaconlaw.ca/new-data-breach-reporting-rules/> (consulted on April 1, 2020)

BELL, S., "Your privacy rights, GDPR and smart devices", *BULLGUARD BLOG*, December 11, 2017, online: <https://www.bullguard.com/blog/2017/12/your-privacy-rights,-gdpr-and-smart-devices> (accessed on October 20, 2019)

BENNETT, K. L., and Jordan MICHAUX, "Canada: Canada's Digital Charter: The Problem Of Trust In A Growing Digital World", *MONDAQ*, June 19, 2019, online: <https://www.mondaq.com/canada/Privacy/816656/Canada39s-Digital-Charter-The-Problem-Of-Trust-In-A-Growing-Digital-World> (accessed on April 6, 2020)

BOUTILIER, A., "New 'digital charter' to emphasize Canadians' control over personal data", *THE STAR*, May 21, 2019, online: <https://www.thestar.com/politics/federal/2019/05/21/new-digital-charter-to-emphasize-canadians-control-over-personal-data.html> (accessed on April 6, 2020)

BOYD, A., "Could your Fitbit data be used to deny you health insurance?", *THECONVERSATION*, February 17, 2017, online: <http://theconversation.com/could-your-fitbit-data-be-used-to-deny-you-health-insurance-72565> (consulted on February 11, 2020)

BROWN, J., "Data fit for the courtroom?", *CANADIAN LAWYER*, February 2, 2015, online: <https://www.canadianlawyermag.com/author/jennifer-brown/data-fit-for-the-courtroom-2765/> (accessed on October 22, 2019)

BURANYI, S., "The WHO v coronavirus: why it can't handle the pandemic", *THE GUARDIAN*, April 10, 2020, online: <https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-v-coronavirus-why-it-cant-handle-pandemic> (consulted on April 24, 2020)

BURKE, D., "Why it is important to outsmart the smart devices", *CBC NEWS*, December 28, 2018, online: <https://www.cbc.ca/news/canada/nova-scotia/privacy-smart-speakers-google-amazon-smart-devices-1.4951026> (accessed on October 21, 2019)

CANADIAN CHAMBER OF COMMERCER, "RE: Canadian Chamber of Commerce Submission to OPC Consultation on transfers for processing – Reframed discussion document", August 6, 2019, email sent to Daniel Therrien by Scott Smith, Senior Director Innovation and Intellectual Property Policy of the Canadian Chamber of Commerce, <http://www.chamber.ca/download.aspx?t=0&pid=d6306339-4db9-e911-9508-c3b36535cc0c>

CANADIAN INSITUTE FOR HEALTH INFORMATION, "Health spending in Canada reaches $264 billion", October 31, 2019, online: <https://www.cihi.ca/en/health-spending-in-canada-reaches-264-billion> (accessed on June 20, 2020)

CANADIAN MEDICAL ASSOCIATION, "The Future of Technology in Health and Health Care: A Primer", 2018, online: <https://www.cma.ca/sites/default/files/pdf/health-advocacy/activity/2018-08-15-future-technology-health-care-e.pdf> (accessed on April 29, 2020)

CARNEY, M., "Leave no dark corner", *ABC NEWS*, September 17, 2018, online : <https://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page%3A%20ABC%20Au

stralia-Facebook_Organic&WT.tsrc=Facebook_Organic&fbclid=IwAR1eiJG-W3lCnyM6A1a0htPIatxwjOQDCj9YEUe4GZZ9WODFCJKqbOjIhEg> (accessed on October 19, 2019)

CASIANO, L., "California man, 91, linked to stepdaughter's death by Fitbit device dies", *FOX NEWS*, September 12, 2019, online: https://www.foxnews.com/us/91-year-old-linked-to-stepdaughters-death-by-fitbit-device-dies> (consulted on October 24, 2019)

CENTER FOR DISEASE CONTROL AND PREVENTION, "Defining Adult Overweight and Obesity", June 30, 2020, online: <https://www.cdc.gov/obesity/adult/defining.html> (accessed on July 25, 2020)

CHRISTOFF, M. C., "United States: Pacemaker Data May Be Smoking Gun In Aggravated Arson Case", *SEYFARTH SHAW*, February 22, 2017, online: <http://www.mondaq.com/unitedstates/x/570222/Civil+Law/Pacemaker+Data+May+Be+Smoking+Gun+in+Aggravated+Arson+Case> (accessed on October 22, 2019)

COLLINS, K., "Google DeepMind's AI can detect over 50 sight-threatening eye conditions: A focus on artificial intelligence could lead to fewer people losing their sight", *CNET*, August 13, 2018, online: <https://www.cnet.com/news/google-deepminds-ai-can-now-detect-over-50-sight-threatening-eye-conditions/> (accessed on October 22, 2019)

CRÊTE, M., "Québec déposera un projet de loi sur la protection des données personnelles", *LE DEVOIR*, September 18, 2019, online : <https://www.ledevoir.com/politique/quebec/562810/quebec-deposera-un-projet-de-loi-sur-la-protection-des-donnees-personnelles> (consulted on April 2, 2020)

CTNT Report, "Cybercrime Tactics and Techniques: the 2019 state of healthcare", November 2019, online: <https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf>

CURATEUR PUBLIC QUÉBEC, "Les droits du mineur", online : <https://www.curateur.gouv.qc.ca/cura/fr/mineur/tutelle-biens/droits/index.html> (consulted on October 29, 2019)

DAVIS, G., "Why Software Updates are so Important", *MCAFEE*, September 17, 2017, online: <https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important/> (consulted on March 26, 2020)

DELOITTE CENTRE FOR HEALTH SOLUTIONS, "Medtech and the Internet of Medical Things | How connected medical devices are transforming health care", July 2018, online: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf> (consulted on March 24, 2020)

DENNE, L., Greg SADLER and Makda GHEBRESLASSIE, "We hired ethical hackers to hack a family's smart home — here's how it turned out", *CBC NEWS*, September 28, 2018, online: <https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963> (accessed on October 27, 2019)

DESROCHERS, A., "Quand des médecins recommandent de porter une montre intelligente", *ICI RADIO-CANADA*, 21 février 2019, online : <https://ici.radio-canada.ca/premiere/emissions/le-15-18/episodes/427492/audio-fil-du-jeudi-21-fevrier-2019/16> (consulté le 27 mars 2019)

DESROCHERS, A., "Quand des médecins recommandent de porter une montre intelligente", *ICI RADIO-CANADA*, February 21, 2019, online : <https://ici.radio-canada.ca/premiere/emissions/le-15-18/episodes/427492/audio-fil-du-jeudi-21-fevrier-2019/16> (accessed on October 27, 2019)

DIBBLE, M., "World Health Organization partners with Google to stop spread of coronavirus misinformation", *WASHINGTON EXAMINER*, February 3, 2020, online: <https://www.washingtonexaminer.com/news/world-health-organization-partners-with-google-to-stop-spread-of-coronavirus-misinformation> (consulted on March 13, 2020)

DOFFMAN, Z., "Ashley Madison Has Signed 30 Million Cheating Spouses. Again. Has Anything Changed?", *FORBES*, August 23, 2019, online: <https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-million-cheating-spouses-signed-since-the-hack/#271a8d803878> (consulted on October 18, 2019)

DOLLY, J., "Why you should never, ever connect to public WiFi", *CSO*, January 9, 2018, online: <https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html> (consulted on March 26, 2020)

DONOVAN, F., "Healthcare Industry Takes Brunt of Ransomware Attacks", *HEALTHITSECURITY*, May 3, 2018, online: <https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks> (consulted on March 20, 2020)

DU PERRON, S., "Projet de loi 64 : une réforme à l'Européenne du droit à la protection des renseignements personnels", *CYBERJUSTICE LABORATORY*, June 17, 2020, online : <https://www.cyberjustice.ca/2020/06/17/projet-de-loi-64-une-reforme-a-leuropeenne-du-droit-a-la-protection-des-renseignements-personnels/> (accessed on July 23, 2020)

DUPOY, D., and Julie HIMO, "New privacy legislation could increase the burden for companies in Quebec", *DATA PROTECTION REPORT*, February 24, 2020, online: <https://www.dataprotectionreport.com/2020/02/new-privacy-legislation-could-increase-the-burden-for-companies-in-quebec/> (consulted on April 1, 2020)

EADICICCO, L., "This Giant Security Hole Could Affect A Huge Chunk Of The 'Secure' Web", *BUSINESS INSIDER*, April 8, 2014, online: <https://www.businessinsider.com/heartbleed-security-flaw-2014-4> (accessed on October 21, 2019)

ÉDUCALOI, "The Right to Access Medical Records", online: <https://educaloi.qc.ca/en/capsules/the-right-to-access-medical-records/> (accessed on July 25, 2020)

ÉPÉE, F., "La protection des données personnelles au Canada à l'ère des données massives", *Laboratoire de CYBERJUSTICE*, July 24, 2018, online : <https://www.cyberjustice.ca/actualites/2018/07/24/la-protection-des-donnees-personnelles-au-canada-a-lere-des-donnees-massives/> (accessed on October 24, 2019)

EUROPEAN COMMISSION, "A new era for data protection in the EU: What changes after May 2018", online: <https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf> (accessed on October 20, 2019)

EVANS, M., "A Primer on the Personal Information Protection and Electronic Documents Act ("PIPEDA") for Pharmaceutical and Medical Device/Technology Companies that Conduct Business in Canada", *LONGWOODS*, 2003, online: <https://www.longwoods.com/content/16404> (consulted on March 26, 2020)

FANCOURT-SMITH, M. E., "Mandatory Data Breach Notification Regime Announced Amid Facebook Scandal", *LAWSONLUNDELL*, April 13, 2018, online: <https://www.lawsonlundell.com/Commercial-Litigation-and-Dispute-Resolution-Blog/mandatory-data-breach-notification-regime-announced-amid-facebook-scandal> (consulted on April 1, 2020)

FEFER, R. F., *Data Flows, Online Privacy, and Trade Policy*, CONGRESSIONAL RESEARCH SERVICE, March 26, 2020, online: <https://crsreports.congress.gov/product/pdf/R/R45584> (consulted on April 7, 2020)

FINDLAW, "Who can access your health records?", online: <https://health.findlaw.ca/article/who-can-access-your-health-records-1/> (consulted on October 28, 2019)

FIONDA, F., "19 million Canadians have had their data breached in eight months", *CTV NEWS*, September 2, 2019, online: <https://www.ctvnews.ca/politics/19-million-canadians-have-had-their-data-breached-in-eight-months-1.4572535> (consulted on April 2, 2020)

Fitbit, "Privacy", online: <https://www.fitbit.com/us/legal/privacy> (consulted on February 11, 2020)

FITBIT, "Fitbit Privacy Policy", September 18, 2018, online: <https://www.fitbit.com/en-ca/legal/privacy-policy> (accessed on October 24, 2019)

FRASER, C., "Target didn't figure out a teenager was pregnant before her father did, and that one article that said they did was silly and bad", *MEDIUM*, January 3, 2020, online: <https://medium.com/@colin.fraser/target-didnt-figure-out-a-teen-girl-was-pregnant-before-her-father-did-a6be13b973a5> (accessed on March 17, 2020)

FRUHLINGER, J., "What is WannaCry ransomware, how does it infect, and who was responsible?", *CSO*, August 30, 2018, online: <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> (consulted on March 19, 2020)

GEIST, M., "Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards", *CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION*, April 4, 2018, online: <https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security> (consulted on October 11, 2019)

GIESECKE, J., "8. International Health Regulations and Epidemic Control", *WORLD HEALTH ORGANIZATION*, online: <https://www.who.int/trade/distance_learning/gpgh/gpgh8/en/index2.html> (consulted on October 25, 2019)

GOVERNMENT OF CANADA, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians", October 23, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html> (accessed on April 6, 2020)

GOVERNMENT OF CANADA, "Canada's Digital Charter: Trust in a digital world", June 25, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html> (consulted on April 2, 2020)

GOVERNMENT OF CANADA, "Canada's Health Care System", online: <https://www.canada.ca/en/health-canada/services/health-care-system/reports-publications/health-care-system/canada.html> (consulted on January 9, 2020)

GOVERNMENT OF CANADA, "Consolidated TPP Text – Chapter 14 – Electronic Commerce", online: <https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng> (consulted on October 11, 2019)

GOVERNMENT OF CANADA, "Fifth Update Report on Developments in Data Protection Law in Canada", June 2019, online: <https://www.ic.gc.ca/eic/site/113.nsf/eng/h_07666.html> (consulted on March 30, 2020)

GOVERNMENT OF CANADA, "Fifth Update Report on Developments in Data Protection Law in Canada", June 2019, online: <https://www.ic.gc.ca/eic/site/113.nsf/eng/h_07666.html> (consulted on March 30, 2020)

GOVERNMENT OF CANADA, "Minister Bains announces Canada's Digital Charter", May 21, 2019, online: <https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/minister-bains-announces-canadas-digital-charter.html> (consulted on April 2, 2020)

GOVERNMENT OF CANADA, "Notice: Health Canada's Approach to Digital Health Technologies", April 10, 2018, online: <https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html> (accessed on May 18, 2020)

GOVERNMENT OF CANADA, "Strengthening Privacy for the Digital Age", May 21, 2019, online: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html> (accessed on April 6, 2020)

GOVERNMENT OF CANADA, "Terms and Conditions", September 19, 2016, online: <https://www.canada.ca/en/public-health/corporate/terms-conditions.html> (accessed on July 24, 2020)

GOVERNMENT OF NEW BRUNSWICK, "New Brunswick Public Service Values and Conduct Guide", online: <https://www2.gnb.ca/content/dam/gnb/Departments/ohr-brh/pdf/other/values_conduct_guide.pdf> (accessed on October 3, 2019)

GOVERNMENT OF YUKON, "Policy 2.27-Privacy Management Policy", October 27, 2015, online: <http://www.atipp.gov.yk.ca/pdf/Privacy-Management-Policy-GAM-FINAL.pdf> (accessed on October 3, 2019)

GRAHAM, C., "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history", *THE TELEGRAPH*, May 20, 2017, online: <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/?subId3=xid:fr1584728850959jff> (consulted on March 20, 2020)

GREENBERG, A., "Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered", *WIRED*, April 17, 2020, online: <https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/> (accessed on May 18, 2020)

HALE, C., "Fitbit for the flu: Researchers show the fitness wearables can help track outbreaks", *FIERCEBIOTECH*, January 17, 2020, online: <https://www.fiercebiotech.com/medtech/fitbit-for-flu-researchers-show-fitness-wearables-can-help-track-outbreaks> (accessed on May 1, 2020)

HAMBLEN, M., "As smartwatches gain traction, personal data privacy worries mount", *COMPUTERWORLD*, May 22, 2015, online: <https://www.computerworld.com/article/2925311/as-smartwatches-gain-traction-personal-data-privacy-worries-mount.html> (accessed on October 21, 2019)

HANCOCK, J., "John Hancock Vitality", online: <https://www.johnhancockinsurance.com/vitality-program.html> (accessed on October 21, 2019)

HARWELL, D., "Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator", *THE WASHINGTON POST*, November 19, 2019, online: <https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/> (accessed on March 27, 2020)

HATMAKER, T., "Users dump AccuWeather iPhone app after learning it sends location data to a third party", *TECHCRUNCH*, 2017, online: <https://techcrunch.com/2017/08/22/accuweather-revealmobile-ios/?ncid=rss> (accessed on October 21, 2019)

HEALTH INFORMATION AND QUALITY AUTHORITY, "WHO Global Health Observatory", online: <https://www.hiqa.ie/areas-we-work/health-information/data-collections/who-global-health-observatory> (consulted on February 17, 2020)

HEYDARI, A., "Cellphone tracking has been used in at least 1 Canadian mall, former employee says", *CBC NEWS*, August 7, 2018, online: <https://www.cbc.ca/news/canada/calgary/cadillac-fairview-mall-location-tracking-1.4775990> (accessed on August 27, 2020)

HILL, K., "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", *FORBES*, February 16, 2012, online: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#210ffc4a6668> (accessed on March 20, 2019)

HOUSE OF COMMONS STANDING COMMITTEE ON HUMAN RIGHTS AND THE STATUS OF PERSONS WITH DISABILITIES, *Privacy: Where do we Draw the Line?*, April 1997, online: <https://www.priv.gc.ca/media/1314/02_06_03d_e.pdf> (consulted on March 27, 2020)

JOHN HANCOCK, "John Hancock Vitality", online: <https://www.johnhancockinsurance.com/vitality-program.html> (accessed on March 21, 2019)

JOLY, Y. and Gratien DALPÉ, "Vers une discrimination génétique au Canada?", *DROIT INC.*, March 19, 2019, online : <http://www.droit-inc.com/article24362-Vers-une-discrimination-genetique-au-Canada?fbclid=IwAR0D-8DEuLHcGAbD0rdIVKUyu16Nevnzt8wzG4wL3GLiw5qDE-ZskdFWsWA> (accessed on October 21, 2019)

JONES, L., Daniele PALUMBO and David BROWN, "Coronavirus: A visual guide to the economic impact", *BBC NEWS*, April 27, 2020, online: <https://www.bbc.com/news/business-51706225> (consulted on April 28, 2020)

KINSA, "Kinsa's Privacy Principle", online: <https://www.kinsahealth.co/privacy-principles/> (consulted on March 19, 2020)

KINSA, "Which Kinsa Thermometer is best for me?", online: <https://www.kinsahealth.com/teladoc/products> (consulted on October 20, 2019)

KNOX, M. P., "Dabate rejects final plea deal", *JOURNALINQUIRER*, January 25, 2019, online: <https://www.journalinquirer.com/crime_and_courts/dabate-rejects-final-plea-deal/article_708b3da6-20c4-11e9-819c-9fc80796d20b.html> (consulted on October 24, 2019)

KRESSER, C., "The Benefits of Using Wearable Technology for Health Tracking", February 7, 2020, online: <https://chriskresser.com/the-benefits-of-using-wearable-technology-for-health-tracking/> (accessed on April 28, 2020)

LANDI, H., "At Augusta University Health, Wearable Technology Enables Real-Time Monitoring of At-Risk Patients", *HEA!THCARE INNOVATION*, April 7, 2017, online: <https://www.hcinnovationgroup.com/clinical-it/article/13028366/at-augusta-university-

health-wearable-technology-enables-realtime-monitoring-of-atrisk-patients> (accessed on December 11, 2019)

LANGLOIS AVOCATS, "2020 : l'année des modifications aux lois canadiennes et québécoises sur la protection des renseignements personnels", January 21, 2020, online : <https://langlois.ca/2020-lannee-des-modifications-aux-lois-canadiennes-et-quebecoises-sur-la-protection-des-renseignements-personnels/> (consulted on April 2, 2020)

LANGONE, A., "We Talked to Security Experts About How to Protect Your Online Data. Here's What They Said", *MONEY*, April 17, 2018, online: <https://money.com/how-to-protect-personal-information/> (consulted on March 26, 2020)

LEGAULT, J. B., "FluWatchers pour surveiller la COVID-19", *LA PRESSE*, April 5, 2020, online : <https://www.lapresse.ca/covid-19/202004/05/01-5268086-fluwatchers-pour-surveiller-la-covid-19.php?fbclid=IwAR2AhGoJGT9MeiYZ6PC3BqlKPu78v4Brb9OQKDNyXZNrxsuzRKgi2VYQIt4> (accessed on May 7, 2020)

LJUNGGREN, D., "Canadian Parliament rushes through ratification of USMCA trade pact", *REUTERS*, March 13, 2020, online: <https://www.reuters.com/article/us-usa-trade-usmca-canada/canadian-parliament-rushes-through-ratification-of-usmca-trade-pact-idUSKBN2102I5> (consulted on March 30, 2020)

LJUNGGREN, D., "Canadian Parliament rushes through ratification of USMCA trade pact", *REUTERS*, March 13, 2020, online: <https://www.reuters.com/article/us-usa-trade-usmca-canada/canadian-parliament-rushes-through-ratification-of-usmca-trade-pact-idUSKBN2102I5> (consulted on March 30, 2020)

MANULIFE, "Get your Apple Watch", online: <https://www.manulife.ca/personal/vitality/vitality-for-individuals/apple-watch.html> (accessed on October 27, 2019)

MCLAUGHLIN, E. C., "Alexa, can you help with this murder case?", *CNN BUISINESS*, December 28, 2016, online: <https://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html> (accessed on October 21, 2019)

MCLAUGHLIN, E. C., "Suspect OKs Amazon to hand over Echo recordings in murder case", *CNN BUISINESS*, April 26, 2017, online: https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html> (accessed on October 21, 2019)

MCNEIL Jr., D. G., "Can Smart Thermometers Track the Spread of the Coronavirus?", *THE NEW YORK TIMES*, March 18, 2020, online: <https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html> (accessed on May 8, 2020)

MILIARD, M., "Scripps, Stanford working with Fitbit to assess wearables' COVID-19 tracking abilities", *HEALTHCAREITNEWS*, April 17, 2020, online: <https://www.healthcareitnews.com/news/scripps-stanford-working-fibit-assess-wearables-covid-19-tracking-abilities> (accessed on Mai 18, 2020)

MILFORD, K., "December 2019: Get Smart! Mitigating Risks in Connected Devices", *EDUCAUSE*, December 17, 2018, online: <https://er.educause.edu/blogs/2018/12/december-2019-get-smart-mitigating-risks-in-connected-devices> (accessed on March 24, 2020)

MILLER, B. and de Lobe LEDERMAN, "Cybersecurity Data Breaches and Mandatory Privacy Breach Reporting: Lessons from Alberta", *BLAKES*, October 18, 2016, online: <https://www.blakes.com/insights/bulletins/2016/cybersecurity-data-breaches-and-mandatory-privacy> (consulted on April 1, 2020)

MINERS, Z., "Google, Facebook, Microsoft show steady rise in surveillance data requests", *COMPUTERWORLD*, February 3rd, 2014, online: <https://www.computerworld.com/article/2487230/google--facebook--microsoft-show-steady-rise-in-surveillance-data-requests.html> (consulted on February 11, 2020)

MINISTRY OF CENTRAL SERVICES, "Cloud Computing Security Policy", December 2018, online: <https://taskroom.sp.saskatchewan.ca/Documents/Cloud-Computing-Security-Policy.pdf> (accessed on October 3, 2019)

MOLLA, R., "People say they care about privacy but they continue to buy devices that can spy on them", *VOX*, May 13, 2019, online: <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security> (accessed on March 13, 2020)

MORAN, P., "How China's 'social credit' system blocked millions of people from travelling", *CBC RADIO*, March 7, 2019, online: <https://www.cbc.ca/radio/thecurrent/the-current-for-march-7-2019-1.5046443/how-china-s-social-credit-system-blocked-millions-of-people-from-travelling-1.5046445> (accessed on August 7, 2020)

MURPHY, H., "Rich People Don't Just Live Longer. They Also Get More Healthy Years", *THE NEW YORK TIMES*, January 16, 2020, online: <https://www.nytimes.com/2020/01/16/science/rich-people-longer-life-study.html> (consulted on February 17, 2020)

NEWMAN, K., "Rooftops, Radio Waves & Your Health Data", in Attention Control with Kevin Newman, *APPLE PODCASTS*, September 9, 2019, at 18:50, online: <https://podcasts.apple.com/ca/podcast/rooftops-radio-waves-you/id1476566791?i=1000449085670> (consulted on April 2, 2020)

NOKIA, "HMD Demystifies Reports About Data Breaches, Spying ECT. On Nokia Phones", *NOKIAMOB*, March 22, 2019, online: <https://nokiamob.net/2019/03/22/hmd-demystifies-reports-about-data-breaches-spying-etc-on-nokia-phones/> (accessed on October 27, 2019)

NORTON, "How to protect your connected wearables", online: <https://ca.norton.com/internetsecurity-iot-how-to-protect-your-connected-wearables.html> (consulted on March 26, 2020)

O'GRADY, K. and Noralou ROOS, "Five things Canadians get wrong about the health system", *THE GLOBE AND MAIL*, September 5, 2014, online: <https://www.theglobeandmail.com/opinion/five-things-canadians-get-wrong-about-the-health-system/article20360452/> (consulted on October 8, 2019)

O"BRIEN, M. and Christina LARSON, "Can AI flag disease outbreaks faster than humans? Not quite", *AP NEWS*, February 19, 2020, online: <https://apnews.com/100fbb228c958f98d4c755b133112582> (consulted on March 17, 2020)

OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, online: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (accessed on October 24, 2019)

OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013, online: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know", October 31, 2019, online: <https://www.priv.gc.ca/en/blog/20191031/> (consulted on April 1, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Agreement between the United States of America, the United Mexican States, and Canada", online: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between> (consulted on January 31, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Announcement: Commissioner concludes consultation on transfers for processing", September 23, 2019, online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/> (consulted on March 30, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Consultation on transfers for processing – Reframed discussion document", June 11, 2019, online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-transfers-for-processing/> (consulted on March 30, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Guidelines for obtaining meaningful consent", May 2018, online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> (consulted on March 30, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Guidelines for processing personal data across borders", January 2009, online: <https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/> (consulted on March 30, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy", 2019, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/> (accessed on May 18, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features", April 4, 2012, online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2012/nr-c_120404/> (consulted on March 26, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts", November 2004, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/> (October 3, 2019)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", May 2011, online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/report_201105/#fn6> (consulted on March 27, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Summary of privacy laws in Canada", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/> (accessed on September 25 2019)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Wearable devices and your privacy", 2017, online: <https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/02_05_d_73_wd/> (accessed on March 27, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Provincial legislation deemed substantially similar to PIPEDA", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/> (accessed on September 25, 2019)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "2018-19 Survey of Canadians on Privacy: Final Report", online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/> (consulted on March 27, 2020)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Guidelines for Overt Video Surveillance in the Private Sector", March 2008, online: <https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gl_vs_080306/> (accessed on March 20, 2019)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Privacy and kids", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/>

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Case for Reforming the Personal Information Protection and Electronic Documents Act", May 2013, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/pipeda_r/pipeda_r_201305/>

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Transferring Personal Information about Canadians Across Borders: Implications of the USA Patriot Act*, August 18, 2004, online: <https://www.priv.gc.ca/media/1296/sub_usapa_040818_e.pdf>

OMRON, "Heart Guide ", online: <https://omronhealthcare.com/products/heartguide-wearable-blood-pressure-monitor-bp8000m/?utm_source=cj&utm_medium=affiliate&cjevent=6166a59f1bc911ea829c01520a24060b> (accessed on December 10, 2019)

OPIE, R., "Smartwatch data helped police make arrest in Adelaide murder case, court hears", *ABC*, March 29, 2018, online: <https://www.abc.net.au/news/2018-03-29/smart-watch-data-helps-police-find-suspect-in-murder-case-court/9602832> (consulted on October 24, 2019)

OPIE, R., "Woman accused of murdering her mother-in-law in Valley View home pleads not guilty", *ABC*, August 23, 2019, online: <https://www.abc.net.au/news/2019-08-23/woman-accused-of-murdering-mother-in-law-pleads-not-guilty/11442382> (consulted on October 24, 2019)

ORSINI, M., "Opinion: Internet of Things poses privacy risks", *MONTREAL GAZETTE*, December 21, 2017, online: <https://montrealgazette.com/opinion/opinion-internet-of-things-poses-privacy-risks> (consulted on October 18, 2019)

OSBORNE, C., "From flu to coronavirus: Smart thermometers deployed to track the spread in real-time", *ZDNET*, March 19, 2020, online: <https://www.zdnet.com/article/smart-thermometers-deployed-to-track-coronavirus-spread-in-real-time/> (accessed on May 8, 2020)

PALMER, D., "Mobile security: These health apps aren't good for your phone or your privacy", *ZDNET*, October 7, 2019, online: <https://www.zdnet.com/article/mobile-security-these-health-apps-arent-good-for-your-phone-or-your-privacy/> (consulted on March 20, 2020)

PAUL, A., "What's the difference between a cold and flu as coronavirus continues to spread?", *METRO*, February 10, 2020, online: <https://metro.co.uk/2020/02/10/whats-the-difference-between-a-cold-and-flu-as-coronavirus-continues-to-spread-12214873/> (consulted on February 11, 2020)

PEREZ, S., "Apple is launching a Research app that will allow US consumers to participate in health studies", *TECHCRUNCH*, September 10, 2019, online: <https://techcrunch.com/2019/09/10/apple-is-launching-a-research-app-that-will-allow-u-s-consumers-to-participate-in-health-studies/> (accessed on December 10, 2019)

PEREZ, S., "Apple Research app arrives on iPhone and Apple Watch with three opt-in health studies", *TECHCRUNCH*, November 14, 2019, online: <https://techcrunch.com/2019/11/14/apple-research-app-arrives-on-iphone-and-apple-watch-with-three-opt-in-health-studies/> (accessed on December 10, 2019)

PEVANS, P., "How bad will Canada's COVID-19 recession be?", *CBC NEWS*, March 27, 2020, online: <https://www.cbc.ca/news/business/covid-19-recession-economy-analysis-1.5510596> (consulted on April 28, 2020)

PHAM, S., "TikTok hit with record fine for collecting data on children", *CNN*, February 28, 2019, online: <https://edition.cnn.com/2019/02/28/tech/tiktok-ftc-fine-children/index.html?fbclid=IwAR2yAZMTgHcd8F7dVuM-A8KvtqFKGlaBMb0LNUfd7SZ1ks_xceeTW4QYTLo> (accessed on May 7, 2020)

PHANEUF, A., "Latest trends in medical monitoring devices and wearable health technology", *BUISINESS INSIDER*, July 19, 2019, online: <https://www.businessinsider.com/wearable-technology-healthcare-medical-devices> (consulted on October 25, 2019)

PHILIPS, "Philips wearable biosensor: Keep watch, know more, respond quickly", online: <https://www.usa.philips.com/healthcare/clinical-solutions/early-warning-scoring/wireless-biosensor> (accessed on December 10, 2019)

PHILIPS, "What is population health management?", online: <https://www.usa.philips.com/healthcare/medical-specialties/population-health/what-is-population-health-management> (accessed on April 29, 2020)

POWELL, N., "Trump signs USMCA, leaving Canada as the last country yet to ratify North American trade deal", *FINANCIAL POST*, January 29, 2020, online: <https://business.financialpost.com/news/economy/trump-signs-usmca-leaving-canada-as-the-last-country-yet-to-ratify-north-american-trade-deal> (consulted on January 31, 2020)

PWC, "The Wearable Life 2.0: Connected Living in a Wearable World", March 2016, online: <https://www.pwc.com/ee/et/publications/pub/pwc-cis-wearables.pdf> (accessed on July 26, 2020)

RANGER, S., "What is the IoT? Everything you need to know about the Internet of Things right now", *ZDNET*, February 3, 2020, online: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/> (consulted on February 24, 2020)

RAO, S., "In today's homes, consumers are willing to sacrifice privacy for convenience", *THE WASHINGTON POST*, September 12, 2018, online: <https://www.washingtonpost.com/lifestyle/style/in-todays-homes-consumers-are-willing-to-sacrifice-privacy-for-convenience/2018/09/11/5f951b4a-a241-11e8-93e3-24d1703d2a7a_story.html> (accessed on April 29, 2020)

RIEGER, S., "At least two malls are using facial recognition technology to track shoppers' ages and genders without telling", *CBC NEWS*, July 26, 2018, online: <https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964> (accessed on August 27, 2020)

RESTA, G., "Human Dignity", *McGill Companion to Law*, June 2015, online: <https://www.mcgill.ca/companion/list/human-dignity> (consulted on January 21, 2020)

REUTERS, "Equifax to pay up to $700 million in US data breach settlement", *CNBC*, July 22, 2019, online: <https://www.cnbc.com/2019/07/22/equifax-to-pay-up-to-650-million-in-data-breach-settlement.html> (consulted on October 18, 2019)

SALINAS, S., "Uber will pay $148 million in connection with a 2016 data breach and cover-up", *CNBC*, September 26, 2018, online: <https://www.cnbc.com/2018/09/26/uber-to-pay-148-million-for-2016-data-breach-and-cover-up.html> (consulted on October 18, 2019)

SCHNEIER, B., "Can Consumers' Online Data Be Protected?", February 14, 2018, online: <https://www.schneier.com/blog/archives/2018/02/can_consumers_o.html> (consulted on March 26, 2020)

SCHROEDER, C., "Resolutions of the ICDPPC", *IAPP*, November 28, 2017, online: <https://iapp.org/news/a/when-the-worlds-dpas-get-together-resolutions-of-the-icdppc/> (accessed on December 18, 2019)

SELADI-SCHULMAN, J., "Flu Facts: Incubation Period and When It's Contagious", *HEALTHLINE*, October 26, 2018, online: <https://www.healthline.com/health/flu-incubation-period> (consulted on February 11, 2020)

SHIPLEY, D., "Equifax data breach a 'digital disaster' for Canadians", *CBC NEWS*, September 17, 2017, online: <https://www.cbc.ca/news/canada/new-brunswick/nb-opinion-equifax-data-breach-1.4293609> (accessed on October 27, 2019)

TAN, S., "How safe is your personal data collected by your smart devices?", *BUSINESS TIMES*, September 18, 2018, online: <https://www.businesstimes.com.sg/opinion/how-safe-is-your-personal-data-collected-by-your-smart-devices> (accessed on March 20, 2019)

THE CANADIAN PRESS, "Uber to inform Canadians affected by data breach Social Sharing", *CBC*, March 9, 2018, online: <https://www.cbc.ca/news/business/uber-breach-data-canadians-1.4570507> (consulted on April 1, 2020)

The Seventy-first World Health Assembly, Res. WHA71.7, (May 26, 2018), online: <http://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf> (accessed on October 28, 2019)

TRUDEL, P., *Le droit de l'information : une introduction*, Montréal, 2017, 17 p., online : <https://pierretrudel.openum.ca/files/sites/6/2017/07/DroitdelinformationINTRO.pdf> (accessed on March 24, 2019)

TVA NOUVELLES, "Des thermomètres intelligents jugés trop indiscrets", October 24, 2018, online : <https://www.tvanouvelles.ca/2018/10/24/des-thermometres-intelligents-juges-trop-indiscrets> (accessed on October 18, 2019)

UNTERSINGER, M., "Le « droit à l'oubli » ne s'applique pas au monde entier, tranche la justice européenne", *LE MONDE*, September 24, 2019, online : <https://www.lemonde.fr/pixels/article/2019/09/24/le-droit-a-l-oubli-ne-s-applique-pas-au-monde-entier-tranche-la-justice-europeenne_6012818_4408996.html> (accessed on October 18, 2019)

VALENTINO-DEVRIES, J., Natasha SINGER, Michael H. KELLER and Aaron KROLIK, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *NY TIMES*, December 10, 2018, online: <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html > (accessed on March 21, 2019)

VANDERKLIPPE, N., "Top Huawei executive says not even Xi Jinping could compel it to help China spy in other countries", *THE GLOBE AND MAIL*, March 26, 2019, online: <https://www.theglobeandmail.com/world/article-top-huawei-executive-says-not-even-xi-jinping-could-compel-it-to-help/> (accessed on October 27, 2019)

WESTMAN, N., "Health Care's Huge Cybersecurity Problem", *THE VERGE*, April 4, 2019, online: <https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation> (consulted on March 20, 2020)

WHITE, G., *Off the Grid: Pinpointing Location-based Technologies and the Law*, PUBLIC INTEREST ADVOCACY CENTRE, June 2015, online: <http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report.pdf> (consulted on March 27, 2020)

WHITTAKER, Z., "Two years after WannaCry, a million computers remain at risk", *TECHCRUNCH*, May 12, 2019, online: <https://techcrunch.com/2019/05/12/wannacry-two-years-on/> (consulted on March 20, 2020)

WILEY, "Impact of the United States-Mexico-Canada Agreement on Data Privacy Rules", November 2018, online: <https://www.wiley.law/newsletter-Nov_2018-PIF-Impact_of_the_United_States-Mexico-Canada_Agreement_on_Data_Privacy_Rules> (consulted on January 28, 2020)

WILLIAMS, R., "Wearables can boost employee productivity by almost 10pc", *THE TELEGRAPH*, May 1, 2014, online: <https://www.telegraph.co.uk/technology/news/10801687/Wearables-can-boost-employee-productivity-by-almost-10pc.html> (accessed on March 21, 2019)

WOOTSON Jr., C. R., "A man detailed his escape from a burning house. His pacemaker told police a different story", *The WASHINGTON POST*, February 8, 2017, online: <https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.d27405b73321> (accessed on October 22, 2019)

WORLD HEALTH ORGANIZATION, "A proposal for increasing the assessed contribution", 2016, online: <https://www.who.int/about/finances-accountability/funding/financing-dialogue/assessed-contribution.pdf> (consulted on April 27, 2020)

WORLD HEALTH ORGANIZATION, "Assessed contributions", online: <https://www.who.int/about/finances-accountability/funding/assessed-contributions/en/> (consulted on April 27, 2020)

WORLD HEALTH ORGANIZATION, "Climate change and human health - risks and responses. Summary", online: <https://www.who.int/globalchange/summary/en/index5.html> (accessed on May 8, 2020)

WORLD HEALTH ORGANIZATION, "Contributors", online: <https://open.who.int/2018-19/contributors/contributor> (consulted on April 27, 2020)

WORLD HEALTH ORGANIZATION, "Global Health Observatory (GHO) data", online: <https://www.who.int/gho/about/en/> (consulted on February 17, 2020)

WORLD HEALTH ORGANIZATION, "Obesity and overweight", February 16, 2018, online: <https://www.who.int/news-room/fact-sheets/detail/obesity-and-overweight> (accessed on October 28, 2019)

WORLD HEALTH ORGANIZATION, "Digital health", online: <https://www.who.int/behealthy/digital-health/promoting-health-in-the-21st-century> (accessed on October 4, 2019)

WORLD HEALTH ORGANIZATION, "Global Health Observatory (GHO) data", online: <https://www.who.int/gho/en/> (accessed on October 28, 2019)

WORLD HEALTH ORGANIZATION, *Managing epidemics: Key facts about major deadly diseases*, May 2018, online: <https://www.who.int/emergencies/diseases/managing-epidemics-interactive.pdf> (accessed on April 28, 2020)

WORLD HEALTH ORGANIZATION, *Programme budget 2020-2021*, May 2019, online: <https://www.who.int/about/finances-accountability/budget/WHOPB-PRP-19.pdf?ua=1> (consulted on April 27, 2020)

WU, K., J., "There are more viruses than stars in the universe. Why do only some infect us?", *NATIONAL GEOGRAPHIC*, April 15, 2020, online: <https://www.nationalgeographic.com/science/2020/04/factors-allow-viruses-infect-humans-coronavirus/> (accessed on May 8, 2020)