Canadian Journal of Law and Technology

Volume 18 | Number 1 Article 2

6-2020

Can PIPEDA 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation against Facial Recognition Technology

Tunca Bolca
University of Ottawa

Can PIPEDA 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation against Facial Recognition Technology

Tunca Bolca*

ABSTRACT

Facial recognition technology is one of the most intrusive and privacy threatening technologies available today. The literature around this technology mainly focuses on its use by the public sector as a mass surveillance tool; however, the private sector uses of facial recognition technologies also raise significant privacy concerns. This paper aims to identify and examine the privacy implications of the private sector uses of facial recognition technologies and the adequacy of Canada's federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), in addressing these privacy concerns. Facial templates produced and recorded by these technologies are types of biometric information. While all biometric information are highly sensitive in nature and require stricter regulatory protections, this paper argues that facial recognition data poses a more significant risk to individuals' privacy and autonomy than other forms of biometric data. First, facial recognition technology can be used on a person from large distances and completely surreptitiously. Second, hiding one's face or avoiding the technology in daily life is hard to accomplish, if not impossible. Third, there is already a vast database of personally identified facial images available in the hands of private organizations, such as social media companies, containing the sensitive data of millions of people ready to be identified. This paper takes the position that PIPEDA does not provide adequate protection of individuals' privacy against facial recognition technologies and significant amendments to the Act are urgently required. Sensitive personal information, which includes facial recognition data, should be defined as a special category of personal information along with stricter protections on their collection, use, retention and disclosure. The role of consent should be re-defined concerning highly sensitive facial recognition data, clear enforcement powers should be given to the Privacy Commissioner of Canada in enforcing the Act and mechanisms to ensure compliance should be regulated in the forms of substantial fines for violations and a private right of action for citizens. However, the paper argues that due to PIPEDA's limited scope of application and constitutional challenges, amending the Act would not be enough to protect all Canadians from the risks this

* LL.B, LL.M (Private Law), LL.M. (Law and Technology, University of Ottawa), CIPP/C. The author would like to thank Professor Teresa Scassa of the University of Ottawa for her helpful comments and feedback, as well as her continuous guidance and support.

technology poses. Accordingly, the paper concludes that along with the proposed amendments to PIPEDA, provincial legislations should also be enacted and enforced to ensure the protection of Canadians' privacy and autonomy against the threats posed by facial recognition technology.
Keywords: facial recognition, biometric, privacy, sensitive personal information, PIPEDA

TABLE OF CONTENTS

INTRODUCTION 52
PART 1 — FACIAL RECOGNITION TECHNOLOGY AND ITS COMMERCIAL USES 56
1.1 The Basics of Facial Recognition Technology 57
1.1.1 Face Detection: "*Is there a face present?*" 57
1.1.2 Characterization: "*What can be inferred from these faces?*" 57
1.1.3 Verification (1-to-1): "*Is this person who he/she claims to be?*" 58
1.1.4 Identification (1-to-many): "*Who is this person?*" 58
1.2 Significance of Facial Recognition Data 61
1.3 Private Sector Uses of Facial Recognition Technologies 63
1.3.1 Characterization: *SceneTap and Mall Cameras* 64
1.3.2 Verification: *FaceID* 66
1.3.3 Identification: *Social Media (Facebook)* 68
PART 2 — FACIAL RECOGNITION TECHNOLOGY AND PIPEDA'S ADEQUACY 71
2.1 Sensitive Personal Information Is Not Defined 72
2.2 Consent is Inadequate 73
2.3 The Scope of PIPEDA is Limited 75
2.4 Oversight and Enforcement Should be Stronger 77
PART 3 — NEW REGULATORY FRAMEWORK FOR THE USE OF FACIAL RECOGNITION TECHNOLOGY 78
3.1 An Examination of Foreign Regulations 80
3.1.1 United States of America (U.S.) 80
3.1.2 Europe (EU) 83
3.2 Amending PIPEDA to Better Protect Canadians 85
3.2.1 Proposed Amendments to PIPEDA 85
3.2.2 PIPEDA's Limited Scope and the Act's Constitutional Challenges 86
3.3 Proposed Provincial Legislation 87
CONCLUSION 89

INTRODUCTION

A password is disposable, interchangeable and vulnerable. Breach of one's ATM code or online banking password, for example, can lead to serious and devastating consequences. However, once it is discovered, you can take control of your account and perhaps even mitigate your losses through legal means. Eventually you can enforce a different, stronger password which you will change

periodically, perhaps start using different authentication tools your institution may offer and move on knowing exactly the damage you suffered and the peace of mind that comes with the awareness that you have stopped any future breaches: you have regained control.

"Your face is your password" said Apple in an advertisement promoting iPhone X and its much anticipated new feature FaceID.[1] If your new password, your face, is compromised, then the above scenario may play out differently. Unless you are in a John Woo movie,[2] you cannot really change your face. Maybe you can alter some little things: facial hair, different hair color, wearing glasses or a hat, however these will not fool technologies such as FaceID.[3] Breach of this password will bring various privacy concerns along with serious risks of identity theft and fraud. Moreover, once it is gone, there is no way to recover, no extra precautions or new "passwords": no way to regain control.

This technology is called facial recognition and is already a part of our lives. Apple's FaceID is just one example and the use of the technology is increasing in both public and private sectors. In the private sector, which will be the focus of this paper, facial recognition technologies are increasingly being adopted by consumers, who appreciate the convenience the technology brings. As a consumer product, the technology is now being implemented in various areas of our lives: in apartment buildings,[4] stores,[5] schools[6] and even in churches.[7]

---

1 "Apple Memory" (9 July 2018), online (video): *Daily Commercials* <dailycommercials.com/apple-memory/>. The same quote can be found in Apple's webpage describing the features of the iPhone. Apple, "Say Hello to iPhone," online: <support.apple.com/en-ca/explore/new-to-iphone>.

2 *Face/Off,* Dir. John Woo, Paramount Pictures, 1997.

3 "Face ID automatically adapts to changes in your appearance, such as wearing cosmetic makeup or growing facial hair ... Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness": Apple, "About Face ID advanced technology" (6 November 2018), online: <support.apple.com/en-ca/HT208108> [Apple, FaceID Technology]. A study in the U.K. by the University of Bradford has found that facial recognition technology works even when only the half of the face is visible: Ali Elmahmudi & Hassan Ugail, "Deep Face Recognition Using Imperfect Facial Data" (2019) 99 Future Generaiton Computer Systems 213.

4 Ginia Bellafante, "The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?" *The New York Times* (28 March 2019), online: <www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html>.

5 U.K. supermarkets use facial recognition software to determine if the shopper is of age to purchase alcohol: Joseph Archer, "Facial Recognition to be Used in British Supermarkets for the First Time" *The Telegraph* (17 October 2018), online: <www.telegraph.co.uk/technology/2018/10/17/facial-recognition-used-british-supermarkets-first-time/>. A Brazilian clothing retailer uses facial recognition tools to monitors customer reactions to clothing items: Angelica Mari, "Brazilian Retailer Quizzed over Facial Recognition Tech" *ZD Net* (13 March 2019), online: <www.zdnet.com/article/brazilian-retailer-quizzed-over-facial-recognition-tech/>; Joseph Pisani, "Coming to Store Shelves: Cameras that Guess Your Age and Sex" *The Associated Press* (23 April 2019), online: <apnews.com/bc0080f3cf4f4eae9f886ec7dfcd5235>. Facial recognition

In the hands of the state, facial recognition technology can become a tool for mass surveillance and poses serious risks for an individual's privacy and autonomy, turning people's lives into a chapter from *1984*.[8] On the other hand, governments rely on the technology for national security purposes as it is a very useful tool for verifying individuals' identity and it is widely used at border and security checks with successful results.[9] However, in the post 9/11 world,

---

tools are being used to track known shoplifters and alert the shopkeepers of their presence in stores: Alfred Ng, "With Facial Recognition, Shoplifting May Get You Banned in Places You've Never Been" *CNET* (20 March 2019), online: < www.cnet.-com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/ > . The technology is also being used for store purchases as shoppers in China have started scanning their faces to make payments in stores: Helen Roxburgh, "Chinese Shoppers Adopt Facial Payments in Cashless Drive" *CTV News* (4 September 2019), online: < www.ctvnews.ca/sci-tech/chinese-shoppers-adopt-facial-payments-in-cashless-drive-1.4576945 > .

6 Issie Lapowsky, "Schools Can Now Get Facial Recognition Tech for Free. Should They?" *Wired* (17 July 2018), online: < www.wired.com/story/realnetworks-facial-recognition-technology-schools/ > .

7 More than 30 churches worldwide are using facial recognition software to track individuals' attendance: Olivia Solon, "Churches Introduce Facial Recognition to Keep Track of Members' Attendance" *Mirror* (17 June 2015), online: < www.mirror.co.uk/news/technology-science/technology/churches-introduce-facial-recognition-keep-5897247 > .

8 George Orwell, *1984* (Toronto: Penguin Books, 1949).

9 Shannon Liao, "New Facial Recognition System Catches First Imposter at U.S. Airport" *The Verge* (24 August 2018), online: < www.theverge.com/2018/8/24/17778736/facial-recognition-washington-airport-immigration-biometric-exit > . U.S. government is planning to deploy facial recognition technologies to 97 percent of departing air passengers by 2023: Emily Birnbaum, "DHS Wants to Use Facial Recognition on 97 Percent of Departing Air Passengers by 2023" *The Hill* (18 April 2019), online: < thehill.com/policy/technology/439481-dhs-wants-to-use-facial-recognition-on-97-percent-of-departing-air > . Regarding the privacy concerns of the use of facial recognition for air or sea travel and the "normalization" of the technology in the eyes of the public, see Ron Hurtibise, "Facial Recognition May Help You Board a Plane Faster. But Should You Worry About Your Privacy?" *The Star* (17 April 2019), online: < www.thestar.com/business/technology/2019/04/17/facial-recognition-may-help-you-board-a-plane-faster-but-should-you-worry-about-your-privacy.html > ; Jason Kelley, "Skip the Surveillance by Opting Out of Face Recognition at Airports" *Electronic Frontier Foundation* (24 April 2019), online: < www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports > ; Allie Funk, "I Opted Out of Facial Recognition at the Airport—It Wasn't Easy" *Wired* (2 July 2019), online: < www.wired.com/story/opt-out-of-facial-recognition-at-the-airport > . Vancouver International Airport became the first airport in Canada to start using this tool: John Hua, "Nexus Users Face New Biometric Scanning Kiosks at Vancouver International Airport" *Global News* (4 November 2019), online: < globalnews.ca/news/6127218/nexus-users-face-new-biometric-scanning-kiosks-at-vancouver-international-airport/ > . Another very promising use of the technology was in India, where it was successful in relocating missing children: The Times of India, "Facial Recognition System Helps Trace 3,000 Missing Children In 4 Days" (22 April 2018), online: < timesofindia.india-

"national security" is an elusive term that raises significant concerns. China's use of this technology provides an example of how facial identification can be tool to undermine basic human rights and create a state of total surveillance.[10] As serious as the privacy concerns public sector use of facial recognition technologies bring, they are outside the scope of this paper.[11]

This paper aims to identify the privacy issues the use of facial recognition technology brings in the private sector and the adequacy of Canada's federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[12] in addressing these concerns. Part I will define and introduce the technology and its uses in the private sector. Part II will examine PIPEDA and identify and evaluate its shortcomings in addressing the privacy concerns that facial recognition technologies raise. Part III will examine

---

times.com/articleshow/63870129.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst>. The Commissioner of the New York Police Department (N.Y.P.D.) has authored an opinion piece at the New York Times explaining the benefits of facial recognition technology, stating that "[i]ts application by the department is carefully controlled and its invaluable contributions to police investigations have been achieved without infringement on the public's right to privacy": James O'Neill, "How Facial Recognition Makes You Safer" *The New York Times* (9 June 2019), online: <https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html>. However, a report by the Center on Privacy & Technology at Georgetown University, which was published just a few weeks before the Commissioner's piece, demonstrated the N.Y.P.D.'s controversial practices with the technology. The report found out that the force used a picture of the famous actor Woody Harrelson in an effort to catch a suspect wanted for larceny due to the fact that the suspect resembled the actor, which was not the first time a celebrity look-alike was used in an effort to identify a suspect through facial recognition: Clare Garvie, "Garbage In, Garbage Out — Facial Recognition on Flawed Data" (16 May 2019), online: <www.flawedfacedata.com>.

[10] BBC News, "China: The World's Biggest Camera Surveillance Network" (25 December 2017), online (video): *YouTube* <www.youtube.com/watch?v=pNf4-d6fDoY>. Chris Buckley, Paul Mozur & Austin Ramzy, "How China Turned A City into A Prison" *The New York Times* (4 April 2019), online: <www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html>. There are also reports claiming that India is seeking to implement a similar facial recognition based surveillance system: Archana Chaudhary, "India Is Planning a Huge China-Style Facial Recognition Program" *Bloomberg* (19 September 2019), online: <www.bloomberg.com/news/articles/2019-09-19/india-seeks-to-adopt-china-style-facial-recognition-in-policing>.

[11] For the public sector uses of the technology and its impact on privacy, see Derek Lai, "Public Video Surveillance by the State: Policy, Privacy Legislation and the Charter" (2007) 45 Alta. L. Rev. 43; Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (2016) *Georgetown Law Center on Privacy & Technology,* online (pdf): <www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>.

[12] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.[*PIPEDA*] or [the Act].

the legal measures taken in different jurisdictions and will make the case for the need of a new regulatory scheme for Canada's private sector privacy protection.

PART I — FACIAL RECOGNITION TECHNOLOGY AND ITS COMMERCIAL USES

While public sector uses of technology as a mass surveillance tool by the state are disturbing to most; the private sector uses of this technology, especially within consumer products, are not only being widely adopted, but also embraced.[13] The digital era has put itself in an indispensable position in our society and changed our understanding and expectations of privacy. Once, we were disturbed by the possible privacy implications of "instantaneous photography,"[14] but now we are very quick to accept the new technologies and start wondering how we were able to survive without them, without thinking about the trade-offs they bring. Langdon Winner argues that technology is not actually serving to address human needs but instead "renovating human needs to match what modern science and engineering happened to make available."[15] The process is on the same course for facial recognition technology. Evan Selinger calls the strategy companies use to get people on board "normalization."[16] He further explains, "[g]et people used to using the technology all the time. Don't

---

[13] In the recent years, the concern of online privacy and the general awareness of privacy issues amongst consumers have been rising, especially in the wake of the Cambridge Analytica scandal. This and other Facebook scandals in 2018 lead to campaigns such as #DeleteFacebook and the backlash was not only towards Facebook, people started to ask questions regarding the data practices of Google and others as well. However, studies have proved that consumers rarely change their online habits as a result of such concerns. Being connected to others, both personally and professionally, is a major part of these platforms and they are indispensible to most. See Tomas Chamorro-Premuzic & Nathalie Nahai, "Why We're So Hypocritical About Online Privacy" *Harvard Business Review* (1 May 2017), online: <hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy>. For the academic studies of consumer behaviour, see Alessandro Acquisti & Ralph Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook" (6th International Privacy Enhancing Technologies Workshop, delivered at Cambridge, U.K., 28-30 June 2006), online: <www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>; Alexander K. Saeri et al., "Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior" (2014) 154 J. Social Psychology 352. Although general awareness might be higher, there is still a long way to go. Another significant study has recently been made in the context of consumer biometric information. The study showed that individuals were willing to provide facial templates and other biometric information to receive perks such as free coffee: Matthew B. Kugler, "From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms" (2019) 10 U.C. Irvine L. Rev. 108.

[14] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193.

[15] Langdon Winner, *The Whale and the Reactor* (Chicago: The University of Chicago Press, 1986) at 170.

[16] Russell Brandom, "How Should We Regulate Facial Recognition?" *The Verge* (29

just make them comfortable with facial recognition technology, engineer the desire for it. Create habits that lead people to believe they can't live without facial recognition tech in their lives. That's what the consumer side of facial recognition technology is doing: making it seem banal and unworthy of concern."[17]

1.1 The Basics of Facial Recognition Technology

Facial recognition is a type of biometric identification that detects and analyses a person's facial characteristics.[18] The technology can be classified in four categories depending on the use and purposes: detection, characterization, verification and identification.

1.1.1 Face Detection: ''Is there a face present?"

Technologies in this category detect the existence of face(s) on a given image. There is no individual-level matching involved with this technology, the system just identifies the presence of a human face in the given image or video.[19] It is widely used in digital photo cameras to detect the presence of faces for automatic focus.[20] The technology is not sophisticated enough to determine any characteristic properties of the face it detects. Considering that there is no identification on any level, the use of face detection technology alone does not raise any privacy concerns.

1.1.2 Characterization: ''What can be inferred from these faces?"

The second category of facial recognition tools analyzes the physical and emotional state[21] of individuals without positively identifying the individual. The

---

August 2018), online: < www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules > .

17 *Ibid.*

18 Future of Privacy Forum , ''Privacy Principles for Facial Recognition Technology" (December 2015) at 2, online: < fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf > [Future of Privacy Forum, ''Principles"].

19 Jesse Davis West, ''Face Detection vs. Face Recognition" *FaceFirst* (28 May 2017), online: < www.facefirst.com/blog/face-detection-vs-face-recognition/ > .

20 Future of Privacy Forum, ''Understanding Facial Detection, Characterization and Recognition Technologies" (March 2018), online: < fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf > .

21 ''Emotional Detection" is now an emerging industry and perhaps can be classified as ''the next stage" in facial recognition technologies. It is current uses include: in schools to detect children's engagement, in job interviews to detect if the candidate is ''a good hire" and in semi-autonomous vehicles for detecting driver attention: Oscar Schwartz, ''Don't Look Now: Why You Should Be Worried About Machines Reading Your Emotions" *The Guardian* (6 March 2019), online: < www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science > ; Saheli Roy Choudhury, ''Amazon Says Its Facial Recognition Can Now Identify Fear" *CNBC* (13 August 2019), online:

technology does not identify the individual, but can determine certain characteristics about the individual, such as age and gender.[22] This technology is mostly used in malls, stores and other entertainment venues that are interested in knowing certain demographic information about their customers.

1.1.3 Verification (1-to-1): ''Is this person who he/she claims to be?"

1-to-1 verification is widely used for authentication purposes. The technology matches the face print of an individual to a previously collected image in order to verify that the present individual is who they claim to be.[23] In this category, the individual submits a biometric template of their face to be verified by the third party. This technology is used in border checks, where the face of the individual present is matched with the biometric data supplied (passports or other forms of biometric identification) and in order to gain secure access to devices or locations such as smartphones and ATMs by matching previously given facial templates.

1.1.4 Identification (1-to-many): ''Who is this person?"

This technology is used to identify unknown individuals by comparing their face prints with an existing database. In 1-to-1 verification, the individual identifies herself (e.g. provides a biometric passport to the border officer) and the system uses that as its ''database" for verifying if the person present has the same biometric face print as the document she provided. However in 1-to-many identification, the individual does not provide any information and generally is not even aware of the existence and use of the technology. Here, the face print acquired by the technology is matched with a database that contains multiple (in most cases, millions) face prints to determine the identity of the individual. The database is constructed through a variety of sources, such as government resources[24] (e.g. driver's licences and other identification pictures) and open

---

< www.cnbc.com/2019/08/14/amazon-says-its-facial-recognition-can-now-identify-fear.html > . It is estimated that the market for ''emotion detection and recognition" will be valued at $92 billion by 2024: Sanjana Varghese, ''The Junk Science of Emotion-Recognition Technology" *The Outline* (21 October 2019), online: < theoutline.com/post/8118/junk-emotion-recognition-technology?utm_source = topic_recent&-zi = qgwfzkkj&zd = 3 > .

22 ''It's a new technology being trotted out to retailers, where cameras try to guess your age, gender or mood as you walk by. The intent is to use the information to show you targeted real-time ads on in-store video screens": Pisani, *supra* note 5.

23 Future of Privacy Forum, ''Principles", *supra* note 18 at 3.

24 In the U.S., it is stated that the F.B.I. has access to 640 million photographs, compiled from driver's licenses, passports and mugshots, that can be searched using facial recognition technology: NBC News, ''Watchdog Says FBI Has Access to about 640M Photographs" (4 June 2019), online: < www.nbcnews.com/news/us-news/watchdog-says-fbi-has-access-about-640m-photographs-n1013751 > . It is estimated that images of half of the American population is already in facial recognition databases: Jake Laperruque et al., ''Facing the Future of Surveillance" *The Project On Government*

sourced online images (e.g. social media and website uploads).[25] Examples of the use of this technology include social media photo tagging suggestions and smart CCTVs used by law enforcement agencies.[26]

Facial recognition systems that are used for 1-to-1 verification or 1-to-many identification purposes use algorithms to scrape essential and differentiating characteristics of an individual's face print. These distinct characteristics, such as the distance between a person's eyes or the shape of their chin, are converted into a mathematical representation, which is called a "face template."[27] The system then uses the face template to find matches in the given database.

There are many reports with different results on the success and accuracy rate of facial recognition technologies.[28] The majority of reports show that the system is still far from perfect and moreover, it is biased against people of colour due to the lack of diverse training sets. A study in 2018 caught worldwide attention where Amazon's Rekognition[29] software was used in the United States

---

Oversight (4 March 2019) at 13-14, online: < s3.amazonaws.com/docs.pogo.org/report/2019/Facing-the-Future-of-Surveillance_2019.pdf > . The law enforcement agencies in Florida are using FACES software that "draws from a database consisting of more than 33 million driver's license and law enforcement photos": Aaron Mak, "Facing Facts" *Slate* (25 January 2019), online: < slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html > . For detailed information on the program and criticisms regarding its use, see Somil Trivedi & Nathan Freed Wessler, "Florida Is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech" *American Civil Liberties Union* (12 March 2019) online: < www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people > .

[25] Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions Of Online Photos Scraped Without Consent" *NBC News* (12 March 2019), online: < www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 > . Social media uploads were also used to construct and train facial recognition algorithms without the consent of users: Olivia Solon & Cyrus Farivar, "Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools" *NBC News* (9 May 2019), online: < www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371 > .

[26] Garvie, Bedoya & Frankle, *supra* note 11 at 27.

[27] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology" *Electronic Frontier Foundation* (12 February 2018) at 5, online: < www.eff.org/files/2018/02/15/face-off-report-1b.pdf > .

[28] Chris Burt, "Facial Recognition 20 Times More Accurate with Advances in Convolutional Neural Networks, NIST Finds" *Biometric Update* (4 December 2018), online: < www.biometricupdate.com/201812/facial-recognition-20-times-more-accurate-with-advances-in-convolutional-neural-networks-nist-finds > ; Big Brother Watch, "Big Brother Watch Response To Planned Police Use Of "Authoritarian" Facial Recognition" (14 December 2018), online: < bigbrotherwatch.org.uk/all-media/big-brother-watch-response-to-planned-police-use-of-authoritarian-facial-recognition/ > .

[29] Amazon Web Services, "Amazon Rekognition" (accessed 1 March 2020), online: < aws.amazon.com/rekognition/?nc1 = h_ls > .

Congress. Rekognition gave 28 "false positive" results,[30] misidentifying the members of the Congress as criminals.[31] The false positive results further demonstrated how Rekoginiton is more accurate with white members of the Congress than other ethnic groups. The false positive results on non-white members were nearly 40%, whereas for white members it was only 5%.[32] The lack of accuracy and the apparent discriminatory results of the technology are deeply disturbing,[33] especially considering the current unregulated uses of facial recognition technologies for 1-to-many identification purposes by law enforcement agencies.[34]

---

[30] A false positive result occurs when the system matches the scanned face to an image at the database incorrectly. A false negative result is received when the system fails to identify a match in the system even though the correct match was in the database.

[31] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots" *American Civil Liberties Union* (26 July 2018), online: < www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 > . Regarding the racial bias in these systems, see Joy Buolamwini, "The Coded Gaze" *Algorithmic Justice League*, online (Youtube): < www.youtube.com/watch?v = 162VzSzzoPs > . A similar study was done in August 2019 by the A.C.L.U. and Rekognition misidentified 26 California lawmakers as criminals: Madeleine Gregory, "Amazon's Facial Recognition Misidentified 1 in 5 California Lawmakers as Criminals" *Vice* (13 August 2019), online: < www.vice.com/en_us/article/ne8wa8/amazons-facial-recognition-misidentified-1-in-5-california-lawmakers-as-criminals > .

[32] AI Now Institute, New York University, "AI Now Report, 2018" (December 2018) at 16, online: < ainowinstitute.org/AI_Now_2018_Report.pdf > .

[33] More than 450 Amazon employees signed a petition for the company to stop developing the company's facial recognition software, Rekognition, and stop supplying it to law enforcement agencies. However, neither this initiative nor media backlash changed Amazon's plans in supplying Rekogition to law enforcement: Nick Statt, "Amazon Told Employees it Would Continue to Sell Facial Recognition Software to Law Enforcement" *The Verge* (8 November 2018), online: < www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations > . Following an M.I.T. study showing that Rekognition has more trouble identifying women and people of colour compared to other facial recognition tools, 25 prominent artificial intelligence scholars signed an open letter to Amazon to stop selling Rekognition to law enforcement agencies: Cade Metz & Natasha Singer, "A.I. Experts Question Amazon's Facial-Recognition Technology" *The New York Times* (3 April 2019), online: < www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html > . In May 2019, Amazon's shareholders voted down a proposal calling for the end of the sale of Rekognition: Colin Lecher, "Amazon Shareholders Vote Down Proposals on Facial Recognition and Climate Change" *The Verge* (22 May 2019), online: < www.theverge.com/2019/5/22/18635632/amazon-shareholders-vote-facial-recognition-climate-change-investors-employees > .

[34] For accuracy concerns of facial recognition tools and racial bias in the public sector, which are not in the scope of this paper, see Garvie, Bedoya & Frankle, *supra* note 11 at 46-57; Lynch, *supra* note 27 at 6-10.

1.2 Significance of Facial Recognition Data

Facial recognition is a form of biometric identification technology.[35] There are several other biometric identification tools such as: voice recognition,[36] fingerprints, eye (retinal) scans, palm scans, vein scans and gait. Due to its nature, unauthorized access to any sort of biometric data is troubling and creates a very high risk of identity theft and fraud as well as serious privacy concerns. After all, biometric information is biologically a part of who we are and thus cannot be altered easily — or at all. Furthermore, the nature of biometric information enables an individual to be personally identified without any need for secondary information, as opposed to other sensitive personal information where having only one piece of information (e.g. having a credit card number but not the name of the card holder) does not always lead to personal identification or becomes a tool for fraud and other malicious activity. Therefore, the collection, use and disclosure of biometric information pose risks warranting stricter privacy protections.

Facial recognition technologies, however, pose an even more significant threat than other forms of biometric data mentioned above. First, as opposed to other biometrics, facial recognition technology can be used on a person from large distances and completely surreptitiously. The collection of other forms of biometric information needs some interaction with the subject (e.g. fingerprints) or needs to happen at least in close proximity of the subject (e.g. voice recognition). As a result, the highly sensitive facial recognition data can be easily collected, in real time, without the subject's awareness. Due to the lack of interaction the data subject may not even be aware of the collection and will not be able to challenge its legality. Second, hiding one's face in public is not an easy task and is even illegal in some states.[37] Advanced cameras with high resolution

---

[35] "The term "biometrics" refers to one or more distinguishing biological characteristic of an individual. A biometric characteristic is a measureable physiological or behavioral trait that may be used to identify an individual": Hannah Zimmerman, "The Data of You: Regulating Private Industry's Collection of Biometric Information" (2018) 66 Kan. L. Rev. 637 at 640.

[36] Voice recognition and analysis tools, combined with machine learning techniques, are being used in healthcare and by private sector entities "to evaluate whether someone is likely to default on a bank loan, buy a more expensive product, or be the best candidate for a job": Angela Chan, "Why Companies Want to Mine the Secrets in Your Voice" *The Verge* (14 March 2019), online: < www.theverge.com/2019/3/14/18264458/voice-technology-speech-analysis-mental-health-risk-privacy > .

[37] Quebec banned the use of face coverings in 2017. France, Austria, Belgium, Germany and Bulgaria also have similar laws banning people from covering their faces: Liam Stack, "Burqa Bans: Which Countries Outlaw Face Coverings?" *The New York Times* (19 October 2017), online: < www.nytimes.com/2017/10/19/world/europe/quebec-burqa-ban-europe.html > . Tunisia, Algeria and Morocco have imposed restrictions on the use of full-face veils and religious coverings for security purposes: Lilia Blaise, "Tunisia Bans Full-Face Veils for Security Reasons" *The New York Times* (5 July 2019), online: < www.nytimes.com/2019/07/05/world/africa/tunisia-ban-veil-niqab.html > .

capabilities are everywhere; attached to lampposts, on drones, in public transport and even integrated on another person's glasses.[38] It is nearly impossible for one to successfully evade the prying eyes of the state or businesses all around.[39] Third, there is already a vast database of facial images available, both in the hands of governments and private companies. Governments collect facial data for identification purposes as it is a strong tool in battling identity fraud. Driver's licence, national ID and passport photos are specifically designed for biometric verification purposes and every resident needs to obtain at least one piece of official identification in order to access most government services, including healthcare. Employment identification records and criminal records are also sources in compiling databases. Although these images are being collected for specified purposes, it is known that law enforcement agencies compile their databases for 1-to-many identification from these images.[40] On the private sector side, social media companies such as Facebook have the largest database of identified images in the world, accompanied with locations and date and time stamps. The existence of these databases prepares an excellent setting for both public and private sector actors to take advantage of the technology: no other biometric identifier has a structured database containing the data of millions of people ready to be identified.[41] These three factors outlined above show that

---

[38] Smart glasses with facial recognition enabled cameras are available for both law enforcement and general public: Jing Zhang, "Glasses with Facial Recognition AI Promise End to Those Awkward Moments When You Forget Someone's Name" *South China Morning Post* (20 January 2018), online: <www.scmp.com/lifestyle/article/2129654/glasses-facial-recognition-ai-promise-end-those-awkward-moments-when-you>.

[39] In an attempt to avoid their faces from being scanned by the technology, protestors in Hong Kong are shining high-powered lasers to security cameras: Kristin Houser, "Hong Kong Protesters Use Lasers to Block Facial Recognition Tech" *Futurism* (2 August 2019), online: <futurism.com/the-byte/hong-kong-protesters-lasers-facial-recognition>. There are a few other attempts to neutralize the technology. One of them is the "Phantom glasses" that bounce back the infrared light back to the surveillance camera to prevent it from capturing a good image of the person's face in real time: Jack Morse, "Fight Facial-Recognition Technology with Phantom Glasses" *Mashable* (12 July 2019), online: <mashable.com/review/review-reflectacles-phantom-anti-facial-recognition-technology-glasses-frames>. Another method is aimed at securing one's face on online streaming platforms. Researchers developed a program called *DeepPrivacy* that anonymizes the individual's face "by masking it with a combination of more than a million other people's faces": Samantha Cole, "This Software Will Give You a Fake Face to Protect Your Privacy" *Vice* (17 September 2019), online: <www.vice.com/en_ca/article/ne87pg/deepprivacy-fake-face-anonymized-algorithm>. An Israeli start-up, D-ID, constructed an anti-facial recognition software "to make organizations' photos and videos unrecognizable to facial recognition tools while keeping them similar to the human eye": D-ID (accessed 3 March 2020), online: <www.deidentification.co>.

[40] Garvie, Bedoya & Frankle, *supra* note 11 at 58.

[41] A recent study once again demonstrated the threats of this technology to anonymity. *The New York Times*, as part of "The Privacy Project," conducted an experiment where a team of researchers turned three security cameras owned by a restaurant that were

facial recognition is amongst one of the most dangerous technologies of surveillance that threatens the privacy of every individual.

1.3 Private Sector Uses of Facial Recognition Technologies

There are countless uses of facial recognition technology in commercial settings. These include: smart TVs that recognize who is watching,[42] gaming devices that recognises and keeps track of the different players,[43] facial recognition-enabled home security systems,[44] dating apps that match people by their facial features,[45] a robot dog that recognizes its owner,[46] ATMs that grant access to accounts via facial recognition tools,[47] targeted billboards,[48] in-store

---

overlooking Bryant Park in New York City to "facial recognition-powered systems" for only $60 and a few days' work. The team ran one day of footage through Amazon's commercial facial recognition service and used only public websites (such as a faculty directory of a university nearby) to positively identify people in the park: Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine" *The New York Times* (16 April 2019), online: <www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html>. Scholars Hartzog and Selinger argue that facial recognition technology has ended public anonymity and obscurity and warn that the other side of obscurity is "chillingly oppressive fear": Woodrow Hartzog & Evan Selinger, "Why You Are No Longer Safe in the Crowd" *The New York Times* (17 April 2019), online: <www.nytimes.com/2019/04/17/opinion/data-privacy.html>. A recent story by *The New York Times* once again proved that unregulated facial recognition technology can end anonymity in public. By scraping photos from the web illegally, New York-based Clearview AI established a database consisting of 3 billion facial images and offered their software to law enforcement agencies in the U.S. It was also discovered that the software included programming language to pair it with augmented-reality glasses, which would enable users to "potentially be able to identify every person they saw. The tool could identify activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew": Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (18 January 2020), online: <www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>. Following this story, a lawsuit was filed in Illinois against Clearview AI: Corinne Reichert, "Clearview AI Sued Over Facial Recognition Privacy Concerns" *CNET* (24 January 2020), online: <www.cnet.com/news/clearview-ai-faces-lawsuit-following-facial-recognition-privacy-concerns/>.

42 Heather Sullivan, "Smart TV offers facial recognition" *NBC* (26 March 2012), online: <www.nbc12.com/story/17257510/smart-tvs-offer-facial-recognition/>.

43 Microsoft Research Blog, "Helping Kinect Recognize Faces" (31 October 2011) online (blog): <www.microsoft.com/en-us/research/blog/helping-kinect-recognize-faces/>.

44 Stephen Mayhew, "Gadspot to Sell Security Cameras with Facial Recognition in North America" *Biometric Update* (10 October 2012), online: <www.biometricupdate.com/201210/gadspot-to-sell-security-cameras-with-facial-recognition-in-north-america>.

45 Huffpost, "Online Dating: Find Your FaceMate Matches Mates By Facial Features" (19 May 2013), online: <www.huffpost.com/entry/online-dating-find-your-f_n_3295087>.

46 Ashley Carman, "Sony's Robot Dog Aibo Is Headed To The US For A Cool $2,899" *The Verge* (23 August 2018), online: <www.theverge.com/2018/8/23/17773084/sony-aibo-dog-us-release-robot>.

personal advertising[49] and many more. This paper will focus on the on the three privacy-relevant categories of the technology outlined above and analyze each with selected examples that will illustrate the specific nature of that category and the privacy concerns it brings.[50]

1.3.1 Characterization: SceneTap and Mall Cameras

Characterization (or classification) is used by establishments like malls and bars to detect and understand certain demographic information about their patrons. The technology itself does not identify the person; however, it detects certain information about a present individual such as gender,[51] age and physical characteristics.

SceneTap was amongst the first applications to use this technology.[52] The app used facial recognition technology to monitor the patrons of a bar or club in order to determine general characteristic information about them, such as the population of a venue and the male/female ratio of the people present,[53] and a patent application in 2012 showed that the app makers were looking to collect more detailed information such as "race, height, weight, attractiveness, hair color, clothing type, and the presence of facial hair or glasses."[54]

---

47 Sarah Kimmorley, "NAB Has Created An ATM That Lets You Withdraw Cash Using Face" *Business Insider* (23 October 2018), online: <www.businessinsider.com.au/nab-atm-facial-recognition-technology-2018-10>.

48 Heather Fletcher, "Facial Recognition: Ads Target Consumers for You" *Target Marketing* (5 October 2015), online: <www.targetmarketingmag.com/article/facial-recognition-ads-target-consumers/all/>.

49 Matt Allegretti, "Facial Recognition Technology Is Turning Heads in Advertising" *Medium* (3 October 2017), online: <medium.com/dumbstruck/facial-recognition-technology-is-turning-heads-in-advertising-3f932c64f21e>.

50 See part 1.1, above. Since the Face Detection category of the technology does lead to the identification of an individual, it does not raise privacy concerns and thus it will not be further analyzed in this paper. The paper will focus on the other three categories of the technology outlined: Characterization, Verification and Identification.

51 A German beer brand, Astra, introduced a smart billboard that uses facial recognition software to scan the individuals passing by and determine their sexes and activate when women are facing it: Benjamin Snyder, "This beer ad only works when women pass by" *Fortune* (21 May 2015), online: <fortune.com/2015/05/21/astra-beer-ad/>.

52 SceneTap later partnered with BarVision: BarVision (accessed 3 March 2020), online: <www.barvision.com/index.php>.

53 The Office of the Privacy Commissioner of Canada, "Automated Facial Recognition in the Public and Private Sectors" (2013) at 3, online: <www.priv.gc.ca/media/1765/fr_201303_e.pdf>.

54 Kashmir Hill, "SceneTap Wants to One Day Tell You the Weights, Heights, Races and Income Levels of the Crowd at Every Bar" *Forbes* (25 September 2012), online: <www.forbes.com/sites/kashmirhill/2012/09/25/scenetap-wants-to-one-day-use-weight-height-race-and-income-to-help-you-decide-which-bar-to-go-to/#5ab0e3fd4acb>.

Recently in Canada, a similar use was discovered and gained considerable media attention. It was discovered that a mall in Calgary, Alberta was using facial recognition technology surreptitiously to collect demographic information on mall goers.[55] This was only discovered due to an error in the mall's directory board which enabled a shopper to see the camera pointed towards him.[56] The mall's application of the technology was done covertly, without any notice to the shoppers and the representatives for the mall defended their practice and claimed that because the cameras only detect age and gender and they do not store any information, they do not require to give notice or to obtain consent.[57] Both the Office of the Privacy Commissioner of Canada (OPCC) and the Office of the Information and Privacy Commissioner of Alberta have started investigating the incident.[58]

The assertion that the technology only collects demographic information and not the identity of the person, does not change the fact that personal information is being collected.[59] PIPEDA's definition of personal information is deliberately broad; any information about an identifiable person is personal information which would include a person's gender or age.[60] Therefore, applications such as *SceneTap* and mall cameras that target individuals who are patrons of a certain establishment are in fact collecting personal information and need to be

---

[55] Sarah Rieger, "At Least Two Malls are Using Facial Recognition Technology to Track Shoppers' Ages And Genders Without Telling" *CBC News* (26 July 2018), online: < www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964 > .

[56] *Ibid.*

[57] Heide Pearson, "Calgary Mall Defends Use of Facial-Recognition Technology After Customer Discovers They're Being Watched" *Global News* (26 July 2018), online: < globalnews.ca/news/4355444/chinook-mall-calgary-facial-recognition-technology/ > .

[58] The Office of the Privacy Commissioner of Canada, "Privacy Commissioner Launches Investigation into Cadillac Fairview Over Use of Facial Recognition Technology in Malls" (3 August 2018), online: < www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180803 > ; The Office of the Information and Privacy Commissioner of Alberta, "Announcement: Commissioner Initiates Investigation Into the Use of Facial Recognition Software at Calgary Malls" (3 August 2018), online: < www.oipc.ab.ca/news-and-events/news-releases/2018/announcement-commissioner-initiates-investigation-into-the-use-of-facial-recognition-software-at-calgary-malls.aspx > .

[59] Aaron Hutchins, "Your Mall is Watching You" *Macleans* (1 November 2018), online: < www.macleans.ca/economy/business/your-mall-is-watching-you/ > .

[60] *PIPEDA*, *supra* note 12 at s. 2(1), "personal information"; Girao v. Zerek Taylor Grossman Hanrahan LLP, 2011 FC 1070, 2011 CarswellNat 3670 (F.C.) at para. 32 ("[I]nformation is personal if it is "about" an identifiable individual. A person will be identifiable if the information disclosed, together with other publicly available information, would tend to or possibly identify them"); The Office of the Privacy Commissioner of Canada, *PIPEDA In Brief* (January 2018), online: < www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_what_is > ("Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: age . . .").

compliant with PIPEDA's rules on notice and consent. Furthermore, even though the information collected does not specifically identify a person by itself (or is later de-identified), a secondary piece of information, gathered from publicly available sources (such as social media profiles) can lead to the identification of that person.[61]

1.3.2 Verification: FaceID

1-to-1 verification is used for authentication purposes. One of the most common uses of facial recognition technology for 1-to-1 verification is for enabling the user access to a password-protected device, account or location. For this purpose, the user will need to first supply the system the initial data and for every subsequent access attempt, the system will use that data to match the present individual's face to make sure that individual is who she says she is. Since the person is actually providing the initial data, the use of this technology does not immediately raise concerns about notice and consent.[62] However, the purposes need to be clearly identified and the extracted facial data should not be used for secondary purposes.

Apple's FaceID was unveiled with its new smartphone, iPhone X, in late 2017.[63] The technology gives the user the convenience of unlocking his or her phone with only a glance, eliminating the need to remember numeric passwords. The use of this technology for the purposes disclosed does not, by itself, create significant privacy threats: the individual is aware and has willingly shared his or her face template with the device. The template is only used to access the device, which is personally used by the individual. However, the possibility of breaches,

---

[61] There are many studies showing that de-identified or anonymized data can easily linked back to the individual using open sourced data: Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701; Michael Barbaro & Tom Zeller, "A Face is Exposed for AOL Searcher No 4417749," *The New York Times* (9 August 2006), online: <www.nytimes.com/2006/08/09/technology/09aol.html>; Arvind Narayanan & Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" (2008) 29th IEEE Symposium on Security and Privacy 111; Yves-Alexandre de Montjoye et al, "Unique in the Crowd: The Privacy Bounds of Human Mobility" (2013) 3 Scientific Reports 1376; Adam Tenner, "Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study" *Forbes* (25 April 2013), online: <www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#1ab1b11992c9>; Olivia Solon, "'Data is a Fingerprint': Why You Aren't as Anonymous as You Think Online" *The Guardian* (13 July 2018), online: <www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy>.

[62] The information can be given involuntarily by an individual as part of unilateral terms of purchase of goods or services. Especially in the health or employment contexts, the individual may be forced to consent to the collection of the identifier. Therefore, although notice is present in such a scenario, the validity of a voluntary and informed consent should also be evaluated in each case in accordance with PIPEDA.

[63] Digital Trends, "Apple iPhone X—Full Announcement from Apple's 2017 Keynote" (12 September 2017), online (video): *Youtube* <www.youtube.com/watch?v=U-my1GN3rlJQ>.

undisclosed secondary uses and unauthorized disclosures pose severe threats to privacy and ruling out these chances is not entirely possible. Apple explicitly states in every occasion that the company does not share the collected face template and that it is not even being stored in an Apple cloud database, it is only stored within the device itself. The company also assures its users that the technology is secure and almost impossible to fool or breach.[64] However, recent history teaches us that any new technology is prone to attacks and none is 100 percent safe.[65] A possible breach of this data has serious consequences.

Another major concern stems from Apple's past practices.[66] Although the company claims it does not share or store the data, its TouchID feature which collected fingerprints (another form of biometric information) does not paint an optimistic picture. TouchID was first released in 2013 with similar promises[67] but in 2015 it was discovered that the company had plans to upload fingerprints to the Cloud.[68] Third party app access is another concern: in 2014 third party apps were given access to TouchID[69] and the company is now doing the same for FaceID.[70] Further, it is known that Apple was one of the companies that shared user personal information with the U.S. National Security Agency's PRISM

---

64 Apple, FaceID Technology, *supra* note 3, "Security safeguards."

65 Raymond Wong, "Hackers Reportedly Bypass Samsung Galaxy S8's 'Airtight' Iris Scanner" *Mashable* (23 May 2017), online: <mashable.com/2017/05/23/samsung-galaxy-s8-iris-scanner-hacked/#kmF4KzIGPmqm>.

66 Recently, Apple has emphasized its privacy practices, using the phrase "What happens on your iPhone stays on your iPhone" and others: Mike Wuerthele, "'Privacy. That's iPhone' Ad Campaign Launches, Highlights Apple's Stance on User Protection" *Apple Insider* (14 March 2019), online: <appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection>. However, a detailed study by the Washington Post revealed that although Apple is more privacy conscious in its own apps and services, the same does not go for third party apps on iPhone, and the 5400 app trackers encountered within one week shows that what happens on your iPhone does not actually stay on it: Geoffrey A. Fowler, "It's The Middle Of The Night. Do You Know Who Your Iphone Is Talking To?" *The Washington Post* (28 May 2019), online: <www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking>.

67 Apple, "Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World" (10 September 2013), online: <www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World/> ("All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it's never stored on Apple servers or backed up to iCloud").

68 Lance Whitney, "Apple Eyes Way To Leave Fingerprints In The Cloud" *CNET* (15 January 2015), online: <www.cnet.com/news/apple-eyes-way-to-sync-your-touch-id-data-in-the-cloud/>.

69 Neil Hughes, "Apple Opens Touch ID to Third-Party Applications with iOS 8" *Apple Insider* (17 September 2014), online: <appleinsider.com/articles/14/09/17/apple-opens-touch-id-to-third-party-applications-with-ios-8>.

70 Geoffrey A. Fowler, "Apple is Sharing your Face with Apps. That's a New Privacy Worry" *The Washington Post* (30 November 2017), online: <www.washingtonpost.-

surveillance program.[71] Therefore, although at this stage Apple claims otherwise, possible invasions of privacy through FaceID may be on their way.[72]

1.3.3 Identification: Social Media (Facebook)

Facial recognition technology is used to personally identify previously unknown individuals. One of the most common uses of identification can be seen in the "Tag Suggestions" of Facebook, which, through its vast database of images and personal information, can identify unknown people in a user's post; even if that person does not have a Facebook account.[73] Facebook's conduct, in both compiling the database and then using it to identify individuals without explicit consent, is a serious invasion of the privacy of those involved.

It is estimated that Facebook has more than 2.3 billion active users.[74] In 2013, it was revealed that 350 million new photos are being uploaded to Facebook daily and that the company has a database of at least 250 billion images.[75] Although the numbers might be less, it is easy to imagine that other

---

com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry/?noredirect = on&utm_term = .872081c61004 > .

71 Sam Gustin, "Tech Companies Jockey To Seem The Most Transparent" *CNN* (18 June 2013), online: < edition.cnn.com/2013/06/18/tech/web/tech-companies-data-transparent/index.html > .

72 These concerns were communicated by U.S. Senator Al Franken in an open letter to Apple. The Senator asked, among other things, whether Apple had any plans to use the facial prints for other purposes and questioned the company's policy regarding law enforcement agencies' requests. However Apple did not specifically address any of the issues raised in the letter but rather repeated the already available online description of the technology: Natasha Lomas, "Apple Responds to Senator Franken's Face ID Privacy Concerns" *Tech Crunch* (17 October 2017), online: < techcrunch.com/2017/10/17/apple-responds-to-senator-frankens-face-id-privacy-concerns/ > ; Kif Leswing, "Apple responds to top senator's privacy questions about the iPhone X's face scanner" *Business Insider* (17 October 2017), online: < www.businessinsider.com/apple-responds-senator-al-franken-privacy-questions-iphone-x-face-id-2017-10 > . Furthermore, in April 2019, it was revealed that a New York student has filed a lawsuit against Apple for $1 billion, claiming that the company's facial recognition software falsely identified him as a suspect in a series of Apple store thefts, which led to his arrest: Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest" *Bloomberg* (22 April 2019), online: < www.bloomberg.com/news/articles/2019-04-22/apple-face-recognition-blamed-by-new-york-teen-for-false-arrest > .

73 In a recent OPCC decision, Facebook's practice of sending emails to non-users of the platform without explicit consent was found to be a violation of PIPEDA and Facebook revised its processes to change this practice: The Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2018-003, "Facebook Agrees To Stop Using Non-Users' Personal Information In Users' Address Books" (24 May 2018), online: < priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-003 > . Using non-users' facial template to identify them without their consent is clearly an even more intrusive and worrisome practice.

74 Zephoria Digital Marketing, "The Top 20 Valuable Facebook Statistics" (March 2019), online: < zephoria.com/top-15-valuable-facebook-statistics/ > .

social media platforms (e.g. Twitter, Snapchat and Instagram, the last of which is also owned by Facebook) have significant amount of identified images. The use of social media in today's world is almost incontestably embedded in our social culture where the refusal to use them can even result in negative reactions from others. Social media companies take advantage of their indispensible nature and keep engaging people to supply them with even more data, no matter if people are aware of how the data is used it or not.[76] Along with the massive facial image database, Facebook also has vast amounts of other information, which enables the company to combine biometric facial information with other important data such as location data and friends, thus making the tech giant's database even more worrisome.

The fact that most images on Facebook are open to the world helps third party apps and others to use them to construct facial databases.[77] A study by Carnegie Mellon University has demonstrated how the profiles on Facebook enabled researchers to identify people walking by.[78] The researchers were able to successfully identify 31% of students walking on campus using only publicly open Facebook profile pictures.[79]

Facebook started using facial recognition technology that has been trained with its massive database for the "Tag Suggestions" feature in 2011.[80] Soon after, Facebook started automatically syncing users' entire photo library to Facebook for the facial recognition technology to classify them for occasions, venues and identify people in the photos which enabled users to share them amongst each other. Later came Moments in 2015,[81] a new Facebook app that was forced upon

---

[75] Cooper Smith, "Facebook Users Are Uploading 350 Million New Photos Each Day" *Business Insider* (18 September 2013), online: < www.businessinsider.com/facebook-350-million-photos-each-day-2013-9 > .

[76] It has been suggested that the "10 Year Challenge" meme that went viral in early 2019 was created by Facebook to obtain a database to train facial recognition algorithms to make better predictions on age progression: Kate O'Neill, "Facebook's '10 Year Challenge' Is Just a Harmless Meme—Right?" *Wired* (15 January 2019), online: < www.wired.com/story/facebook-10-year-meme-challenge/ > .

[77] A Russian App uses open social media databases to enable its users identify people in public: Shaun Walker, "Face Recognition App Taking Russia By Storm May Bring End To Public Anonymity" *The Guardian* (17 May 2016), online: < www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte > .

[78] Allessandro Acquisti, Ralph Gross & Fred Stutzman, "Face Recognition and Privacy in the Age of Augmented Reality" (2014) 6(2) Journal of Privacy and Confidentiality 1.

[79] *Ibid* at 9.

[80] Ben Parr, "Facebook Brings Facial Recognition to Photo Tagging" *Mashable* (15 December 2010), online: < mashable.com/2010/12/15/facebook-photo-tag-suggestions/#uH7xE0CoVZqL > .

[81] Molly McHugh, "Facebook Moments Is A Smarter Photo App—Much Smarter" *Wired* (15 June 2015), online: < www.wired.com/2015/06/facebook-moments/ > .

users[82] and was meant to offer a more convenient way of classifying and organising photos, by the help of its facial recognition system.[83]

Even before Moments was unveiled, Facebook's Tag Suggestions came under fire in the European Union (EU). In 2012, the EU's Article 29 Working Party released an opinion where the tagging feature of Facebook was specifically addressed:

> Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose. If there is a legal basis for this secondary purpose the processing must also be adequate, relevant and not excessive in relation to that purpose. If a data subject has consented that photographs where he appears may be processed to automatically tag him in an online photo album with a facial recognition algorithm, this processing has to be achieved in a data protection friendly way: biometric data not needed anymore after the tagging of the images with the name, nickname or any other text specified by the data subject must be deleted. The creation of a permanent biometric database is a priori not necessary for this purpose.[84]

Following the opinion, complaints were lodged both in Germany and in Ireland, where the company has its European headquarters.[85] As a result of the investigations, Facebook was forced to de-activate its facial recognition technology in Europe and deleted all images captured and identified.[86]

---

[82] A lot of users found out by the threatening emails from Facebook that the pictures on their devices have been being uploaded to Facebook for some time and that they were going to be deleted if the new Moments app was not installed: Sarah Perez, "Facebook Forces its Photo-Sharing App Moments to The Top of the App Store" *Tech Crunch* (10 June 2016), online: < techcrunch.com/2016/06/10/facebook-forces-its-photo-sharing-app-moments-to-the-top-of-the-app-store/ > .

[83] Moments wasn't the success that Facebook imagined it would be and as a result it has been shut down as of February 25, 2019: Richard Nieva, "Facebook is shutting down its Moments app" *CNET* (24 January 2019), online: < www.cnet.com/news/facebook-is-shutting-down-its-moments-photo-app-on-feb-25/ > .

[84] EC, Article 29 Data Protection Working Party, "Opinion 3/2012 on developments in biometric technologies" (00720/12/EN-WP193) at 7, online: < ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf > .

[85] Kevin J. O'Brien, "Germans Reopen Investigation on Facebook Privacy" *The New York Times* (15 August 2012), online: < www.nytimes.com/2012/08/16/technology/germans-reopen-facebook-privacy-inquiry.html > .

[86] Adi Robertson, "Facebook Deletes European Facial Recognition Data, Satisfying German Privacy Agency" *The Verge* (7 February 2013), online: < www.theverge.com/2013/2/7/3964550/facebook-deletes-european-facial-recognition-data > . There are recent reports that Facebook has decided to discontinue Tag Suggestions and instead the technology will be available to all customers with an ability to opt-out: Emily Birnbaum,

PART 2 — FACIAL RECOGNITION TECHNOLOGY AND PIPEDA'S ADEQUACY

Canada's Act for the protection of personal information in the private sector, PIPEDA, came into force on January 1, 2001.[87] It was enacted in response to EU's Data Protection Directive of 1995,[88] in order to maintain the data flow across the Atlantic.[89] Although there were some criticisms,[90] the EU declared that PIPEDA was adequate for the purposes of the Directive.[91]

PIPEDA governs the protection of personal information in the private sector throughout Canada, with the exception of British Columbia, Alberta and Quebec. These three provinces have their own private sector legislations[92] that are "substantially similar" to PIPEDA.[93] Therefore, the private sector actors in these provinces are bound by their respective acts and PIPEDA is not applicable to them.[94]

PIPEDA has been criticized by the privacy community for years but the call for significant amendments to the legislation has so far been ignored by the

---

"Facebook Ends Facial Recognition Photo Tagging Suggestions" *The Hill* (3 September 2019), online: < thehill.com/policy/technology/459771-facebook-ends-facial-recognition-photo-tagging-suggestions > . However, privacy scholars are still not content with Facebook's practices regarding facial recognition technology: Evan Selinger, "Why You Can't Really Consent to Facebook's Facial Recognition" *Medium* (30 September 2019), online: < onezero.medium.com/why-you-cant-really-consent-to-facebook-s-facial-recognition-6bb94ea1dc8f > .

87 PIPEDA's Part 1, which regulates protection of personal information and thus is the focus of this paper, came into force at the given date. Parts 2-5 of PIPEDA came into force on different dates, but are not in the scope of this paper. See *PIPEDA, supra* note 12 at s. 72.

88 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ L281/31 [*Directive*].

89 Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy In Canada* (Toronto: Thomson Reuters, 2018) at 4-4.

90 EC, Article 29 Data Protection Working Party, "Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act" (5109/00 —WP39), online: < ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf > .

91 EC, *Commission decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act,* [2001] OJ, L2/13.

92 *Personal Information Protection Act*, S.B.C. 2003, c. 63 [*BC-PIPA*]; *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [*AB-PIPA*]; *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1.

93 The requirements for being accepted as "substantially similar" have been published by Industry Canada: Department of Industry, *Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council* (2002), C Gaz I, 2385.

94 *PIPEDA, supra* note 12 at ss. 26 (2)(b).

government.[95] PIPEDA's shortcomings are problematic in the context of facial recognition technologies and it is not adequate in protecting the biometric information of Canadians. Biometric and other sensitive information are not defined in the Act and there are no special provisions to protect this vital data. The constitutional restrains on the scope of PIPEDA means that it cannot extend to employees within provincial jurisdiction, limiting its usefulness in curbing the use of facial recognition technologies in the workplace. The consent-based model of PIPEDA has proven to be inadequate in handling highly sensitive information. The OPCC, which provides oversight to the Act, does not have order-making powers, which causes ineffective enforcement. These and other points, which are detailed below, demonstrate that PIPEDA is inadequate in protecting Canadians from the risks of facial recognition technologies.

2.1 Sensitive Personal Information Is Not Defined

Facial recognition data (as well as other forms of biometric data) contains highly sensitive information. PIPEDA's principles differentiate sensitive and less sensitive data, but the Act does not expressly define what constitutes sensitive personal information. Principle 4.3.4 of the Act gives an interpretation of sensitive information, indicating that any information can be sensitive in a given context. Medical and financial information are almost always considered to be sensitive personal information. Principle 4.3.6 states that express consent should be sought when the information is considered sensitive. Finally, principle 4.7.2 states that sensitive information should be safeguarded by a higher level of protection.

PIPEDA defines that any information can be sensitive, so that the information can be evaluated for sensitivity in each case, as other considerations are crucially important in such an evaluation. Principle 4.3.4 gives the example of a magazine subscription, and states that the names and addresses on a newsmagazine would generally not be considered to be sensitive information but names and addresses of subscribers of a special-interest magazine, for example with adult content, is considered sensitive. Although this approach is useful in the given example, facial recognition data needs to be defined explicitly as sensitive personal information, without the need for interpretation. Due to its nature and potential secondary uses, facial recognition data is one of the most vulnerable categories of personal information available, however other biometric data also have similar risks

---

[95] The OPCC reiterated its call for amendments on its annual report to the government: The Office of the Privacy Commissioner of Canada, "2017-18 Annual Report to Parliament" (2018) at 2, online: <www.priv.gc.ca/media/4831/ar_201718_eng.pdf> [2017-18 Annual Report]; see also House Of Commons, Standing Committee On Access To Information, Privacy And Ethics, *Towards Privacy By Design: Review of the Personal Information Protection and Electronic Documents Act* (February 2018), online: <www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>.

and considerations that warrant concern and require extra protection. In 2011, the OPCC found that a woman's complaint regarding the collection of her biometric information (palm and vein scan), which was also to be disclosed to a third party in the U.S., solely for the purposes of authenticating her identity for an exam was not well-founded. One of the OPCC's reasons in reaching this conclusion was that palm-vein scan was "not overly sensitive information."[96] OPCC's interpretation of facial recognition data might differ, but this decision and similar others[97] demonstrate that even biometric information can be interpreted as non-sensitive. This is a dangerous precedent over the status of all biometrics, including facial recognition data. Accordingly, facial templates should be defined in legislation as sensitive information in order to prevent such fraught interpretations that can lead to irrevocable privacy violations.

2.2 Consent is Inadequate

PIPEDA requires informed consent for the collection, use and disclosure of personal information.[98] Section 7 of the Act defines the exceptions to this rule for collection, use and disclosure, where consent of the individual is not required. Principle 3 of Schedule 1 further defines consent and the appropriate practices to obtain consent. According to principle 4.3.6, organizations should "generally" seek express consent but can settle with implied consent if the information is not sensitive.

Giving notice to the individual for collection and acquiring the individual's express consent is very hard to achieve when it comes to facial recognition technologies. The high technology cameras can capture images from long distances and thus in most cases there is no notice or consent at all and the collection is done surreptitiously. In other cases, a notice is given and the individual is deemed to have given her implied consent because she is informed of the collection and decided to be present at the given location. This is mostly the case with regard to malls, bars and other entertainment venues where facial recognition is used for characterization and classification purposes.[99] Even though principle 4.3.6 allows implied consent when the information is "less sensitive," the lack of definition of sensitive information creates a problem. An interpretation like the OPCC's, where biometric information is considered "not overly sensitive information"[100] creates the opportunity for facial recognition

---

[96] PIPEDA Case summary No. 2011-012, Re, 2011 CarswellNat 6894 (Can. Privacy Commr.) [*2011-012*].

[97] The OPCC found that voice prints, which were collected from employees for granting access to a computer network, "does not tell much about the individual." That case was brought to Federal Court which approved the OPCC's decision, which was then affirmed by the Federal Court of Appeal: Turner v. Telus Communications Inc., 2005 FC 1601, 2005 CarswellNat 3954 (F.C.) at para. 22, affirmed 2007 FCA 21, 2007 CarswellNat 172 (F.C.A.) [*Turner v. Telus Communications*].

[98] *PIPEDA, supra* note 12 at Schedule 1, principle 4.3.

[99] See part 1.3, above.

technologies to be used with the implied consent of the subjects. The risk that facial recognition data poses justifies the complete and explicit ban of businesses relying on implied consent. The use of this technology should require express consent.[101]

It is very important how the businesses that use the technology for characterization and classification purposes will handle customers who do not want to give their consent for the use of this technology. A "take-it-or-leave-it" approach is unacceptable. PIPEDA prohibits practices of "forced consent": principle 4.3.3 states that organizations can't require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. However, the OPCC decision mentioned above[102] showed that biometric scan for 1-to-1 verification purposes did not meet the requirements of this principle. Even though there were many other security measures that could have been used and thus the collection of the biometric data was not needed to supply the actual service, the individual was forced to consent to this collection and disclosure because she needed to take the exam. The mall in Alberta used the technology for characterization purposes without notice.[103] Some other malls are giving notice, but are not obtaining consent of mall-goers.[104] If the individual is opposed to the use of the technology and the establishments do not allow the individual to decline participation, the individual will either have to forego consent and subject herself to monitoring despite not consenting to it, or will be forced to take her business elsewhere, where possible. At the end of the day, if every supermarket has digital signs for the purposes of characterization and personalized ads, individuals would eventually have to surrender to the technology. Therefore, it is important that

---

[100] *2011-012*, *supra* note 96.

[101] Another important issue arises in third party interactions with these systems, especially in home electronics, where the owner consents the use of facial recognition technologies, for example within home security systems, but his/her guests are not aware of these tools. In such cases facial templates of third parties will be collected by the company without their consent and as the Supreme Court of Canada decided in *R. v. Reeves*, 2018 SCC 56, 2018 CarswellOnt 20930 (S.C.C.) at paras. 50-52, the owner's consent in processing a third party's data will not be valid. Some companies are trying to use terms and conditions to shift the blame to the owners of the technology, which is problematic and unenforceable. The home security system producer Nest instructs its users that "[d]epending on where you live and how you configure the Products and Services, you may need to get explicit consent to scan the faces of people visiting your home" and Sony's facial recognition enabled robot dog Aibo comes with a manual that mandates that "Each Aibo Product owner further agrees that (s)he will obtain a similar consent from any person who (s)he allows in proximity to or to interact with his or her Aibo Product": Molly Price, "Smart Home Cameras Bring Facial Recognition Ethics To Your Front Door" *CNET* (2 April 2019), online: < www.cnet.com/news/smart-home-cameras-bring-the-facial-recognition-ethical-dilemma-to-your-front-door/ > .

[102] *2011-012*, *supra* note 96.

[103] Rieger, *supra* note 55.

[104] Hutchins, *supra* note 59.

legislation specifically bans the use of digital signs and other facial recognition tools as a condition of access to businesses' products or services, unless the main and identified purposes of the business requires this technology.

Furthermore, it has been argued that the idea of informed consent as a basis for real user control over data is a failure.[105] Hartzog makes the point that everyday users cannot possibly understand the privacy practices they consent to and that users are being tasked with "an impossibly complex calculation to make about future risks and consequences."[106] Reliance upon a meaningful and informed consent, especially for the collection, use and disclosure of sensitive personal information might not be the best legal approach to be taken in a data protection regulation.[107] A regulation with a stricter consent regime and a more paternalistic approach, where certain uses of the technology are not applicable on the basis of user consent but are banned by legislation, is a better approach to protect the society in general. As Zeynep Tufekci puts it, "[d]ata privacy is not like a consumer good, where you click "I accept" and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices."[108]

2.3 The Scope of PIPEDA is Limited

PIPEDA applies to every organization that collects, uses or discloses personal information in the course of commercial activities.[109] The Act also applies to personal information of employees of organizations that collect, use or disclose personal information in connection with the operation of a federal work, undertaking or business.[110] As a result, some individuals, for example an

---

[105] Woodrow Hartzog & Evan Selinger, "Facial Recognition Is the Perfect Tool for Oppression" *Medium* (2 August 2018), online: <medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>. Scholars Woodrow Hartzog and Evan Selinger have been advocating for a complete ban of facial recognition technologies. They call the technology "the most uniquely dangerous surveillance mechanism ever invented."

[106] Woodrow Hartzog, "User Agreements Are Betraying You" *Medium* (5 June 2018), online: <medium.com/s/trustissues/user-agreements-are-betraying-you-19db7135441f>. Helen Nissenbaum also believes that consent is not the solution and does not work: Scott Berinato, "Stop Thinking About Consent: It Isn't Possible and It Isn't Right" *Harvard Business Review* (24 September 2018), online: <hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right>.

[107] *The New York Times* Editorial Board, "How Silicon Valley Puts the 'Con' in Consent" *The New York Times* (2 February 2019), online: <www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html>.

[108] Zeynep Tufekci, "The Latest Data Privacy Debacle" *The New York Times* (30 January 2018), online: <www.nytimes.com/2018/01/30/opinion/strava-privacy.html>.

[109] *PIPEDA, supra* note 12 at s. 4(1)(a).

[110] *PIPEDA, supra* note 12 at s. 4(1)(b).

employee of a business that does not operate in connection with a federal work or undertaking, are not within the scope of the Act.

The limited scope of PIPEDA creates significant risks for certain individuals, especially in the employment context. Companies have been using biometric technologies for verification purposes in the workplace for some time; voice recognition systems for accessing a computer network[111] and fingerprint scanning[112] or hand scanning[113] devices for recording attendance are a few examples. Facial recognition tools are not far behind. Private companies, such as *Alibaba*, have been using these systems for granting workers access to their facilities and other verification purposes.[114] Seeing the worldwide interest in facial recognition, it can be easily deduced that more and more businesses will replace their existing time cards with these technologies in Canada and PIPEDA will not be applicable in protecting employees (whose employers are not federally regulated) from the technology or from ensuring that the technology is being used in accordance with law.[115]

---

[111] *Turner v. Telus Communications, supra* note 97. In this case, the Federal Court of Appeal examined Telus' use of voice recognition tools for granting employees access to the secure computer network. The Court approved Telus' use of the technology, as the Court believed that voice prints were not sensitive information. The Court also considered the fact that there were safeguards present, the company had reasonable business interests, collection of voice prints were reasonable in terms of cost and benefits in comparison with other measures that could have been taken and finally that the loss of privacy was proportionate to the benefit gained.

[112] *IKO Industries Ltd. v. U.S.W.A., Local 8580*, 2005 CarswellOnt 3690, 140 L.A.C. (4th) 393 (Ont. Arb.). In this Ontario case, the Arbitrator concluded that fingerprint scanning system of the employer posed an invasion of privacy of the employees and that the company could not justify its use. However, in a similar arbitration case, *Agropur Division Natrel v. Teamsters, Local 647*, 2008 CarswellOnt 8670, 180 L.A.C. (4th) 252 (Ont. Arb.), the arbitrator concluded that fingerprint scans did not constitute an invasion of privacy of the employees and that the company had established legitimate business reasons.

[113] *Canada Safeway Ltd. v. U.F.C.W., Local 401*, 2005 CarswellAlta 2088, [2005] A.G.A.A. No. 109 (Alta. Arb.). In this arbitration case, the employer introduced a hand scanning system to verify the identities of the employees and record their time of entrance and exit from the workplace. The Arbitrator held that the hand scanning system was justified because; i) method of collection was not intrusive, time consuming or painful, ii) the personal information was kept as templates and did not reveal information about the characteristics of the individual, iii) the template is not completely unique (had up to 1% error rate) and iv) there were adequate protection mechanisms.

[114] Alibaba Tech, "Enter Your Username and Say Cheese: Facial Recognition in Practice at Alibaba" *Medium* (20 August 2018), online: <medium.com/coinmonks/enter-your-username-and-say-cheese-facial-recognition-in-practice-at-alibaba-18820b0d758c>; Mike Rogoway, "Intel Starts Using Facial Recognition Technology to ID Workers, Visitors" *Oregon Live* (11 March 2020), online: <www.oregonlive.com/silicon-forest/2020/03/intel-starts-using-facial-recognition-technology-to-scan-workers-visitors.html>.

[115] In Alberta, British Columbia and Quebec, which have their own provincial private sector privacy legislation, employees of provincially regulated businesses are also protected as

Moreover, the definition and interpretation of "commercial activity" has also been a subject of debate. Should the organization be operating for profit to be classified as engaging in commercial activity? What about non-profit organizations?[116] A judge ruled that collection of personal information by an investigator for the purposes of gathering evidence for a civil suit did not constitute commercial activity,[117] but a physician's examination of an individual for an insurance claim was ruled to be commercial activity.[118] The OPCC has issued guidelines[119] to help with the determination of an organization's status, but the term can be interpreted differently in particular contexts, therefore possibly narrowing the scope of the Act. The significant and unique threats posed by this technology justify a regulatory scheme that is applicable to any and all private organizations in Canada to ensure that protection extends to every resident of Canada.

2.4 Oversight and Enforcement Should Be Stronger

The OPCC is charged with oversight of PIPEDA and has some powers that enable it to push for compliance with the Act. The Commissioner receives complaints and conducts investigations with substantial powers. However, the Commissioner does not enjoy the same level of powers for enforcement. The OPCC can only issue findings and recommendations and does not have the power to order compliance. The matter can be taken to the Federal Court either by the complainant or the OPCC in certain circumstances after the OPCC has issued its report.[120]

The fact that the OPCC does not have order-making powers limits its ability to exercise a meaningful oversight on PIPEDA. The Commissioner has been

---

they are exempt from applying PIPEDA. However, these acts also do not specify sensitive information and thus have their shortcomings in protecting their citizens from the collection, use and disclosure of facial recognition and other biometric information.

[116] Kris Klein & Aron Feuer, *Canadian Privacy: Data Protection Law and Policy for the Practitioner,* 3rd ed. (Portsmouth, U.S.A.: International Association of Privacy Professionals, 2018) at 42.

[117] *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)*, 2010 FC 736, 2010 CarswellNat 2225 (F.C.).

[118] *Rousseau v. Wyndowe*, 2008 FCA 39, 2008 CarswellNat 246 (F.C.A.); Klein & Feuer, *supra* note 116 at 43.

[119] The Office of the Privacy Commissioner of Canada, "Commercial Activity" (January 2017), online: <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/>. The OPCC also issued guidelines for non-profit organizations: The Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Charitable and Non-Profit Organizations" (Revised June 2019), online: <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_19/>.

[120] *PIPEDA, supra* note 12 at s. 14 &15.

advocating for stronger powers in enforcement for some time and privacy advocates agree.[121] However, the Commissioner has also been criticized about the office's lack of use of the current powers, however limited they might be.[122] PIPEDA's section 16 allows the Federal Court to issue damages and fines. However, due to the lack of cases that make its way to the Court and the Court's extremely conservative nature in awarding damages, this mechanism is far from being deterrent.[123] A regulation protecting sensitive information such as facial recognition data should include serious fines for non-compliance that will have a deterrent effect on organizations.[124]

PART 3 — PROPOSAL FOR A NEW REGULATORY FRAMEWORK FOR THE USE OF FACIAL RECOGNITION TECHNOLOGY

This paper has taken the viewpoint that facial recognition technology is one of the most invasive technologies when it comes to an individual's privacy and autonomy.[125] The fact that the technology can be implemented remotely, secretly, cheaply and automatically demonstrates its significance and its difference from other privacy threatening technologies, even from other forms

---

[121] 2017-18 Annual Report, *supra* note 95. Order making powers are given to the provincial commissioners by their private sector legislation in British Columbia (*BC-PIPA*, *supra* note 92 at s. 52) and Alberta (*AB-PIPA*, *supra* note 92 at s. 52), which strengthens the position of the OPCC in its demand.

[122] Michael Geist, "A Failure of Enforcement: Why Changing the Law Won't Fix All That Ails Canadian Privacy" (7 December 2018), online (blog): < www.michaelgeist.ca/2018/12/privacyenforcement/ > .

[123] Additionally, the financial burden and access to justice issues in Canada are other barriers for complainants that reduce the effectiveness of the Federal Court process.

[124] Canadian Anti-Spam Legislation, CASL, regulates commercial electronic messages and prohibits spams to be sent to consumers unless the necessary consent has been obtained in accordance with the legislation. For violations CASL, individuals can be fined up to $1 million and corporations up to $10 million: *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23, s. 20(4). A business that disclosed sensitive financial information without consent, which also led to financial loss for the plaintiff, was fined $5.000 for the privacy violation: Nammo v. Transunion of Canada Inc., 2010 FC 1284, 2010 CarswellNat 4908 (F.C.). If the same business were to send unsolicited commercial messages to that same client, it might have been fined hundreds of thousands of dollars or even more under CASL. Considering the potential harms to the victims of the two scenarios, it is clear that there is an imbalance that needs to be addressed. In 2015, a Quebec company was fined $1.1 million for sending unsolicited emails: CBC News, "Compu-Finder fined $1.1M under anti-spam law" *CBC* (5 March 2015), online: < www.cbc.ca/news/technology/compu-finder-fined-1-1m-under-anti-spam-law-1.2983171 > .

[125] See part 1.2, above.

of biometric data. Our faces are automatically accessible to society and exposed in public, which gives us more reasons to be protective of them. This automatic accessibility also means that we cannot possibly prevent others from capturing our images and subjecting us to facial recognition tools at all times.[126] These points and others made throughout this paper strongly indicate the need for the regulatory protection of the public from the implementation of facial recognition technologies.[127]

Implementation of the technology is increasing every day and the technology will get out of stores, malls and workplaces to the streets, becoming an always-on and ubiquitous technology. The risks the technology poses led even technology companies to warn regulators and society of its dangers, which is unprecedented.

---

[126] Adam Schwartz, "The Danger of Corporate Facial Recognition Tech" *Electronic Frontier Foundation* (7 June 2016), online: < www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-tech > .

[127] The implementation of facial recognition technology is worldwide, and considering the severe threat of mass surveillance of individuals that certainly undermines an individual's autonomy, it can be argued that the issue should be governed in an international setting. In fact, it is a human rights issue that is directly affecting people's dignity and freedom. Article 12 of the Universal Declaration of Human Rights specifically protects individuals' privacy: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks": *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71 at 12. The acceptance of privacy as a human right was restated in the International Covenant on Civil and Political Rights in 1966: *International Covenant on Civil and Political Rights*, 16 December 1966, 999 UNTS 171 at 17 (entered into force 23 March 1976, accession by Canada 19 May 1976). The International Conference of Data Protection & Privacy Commissioners recently accepted a resolution encouraging governments to recognize privacy as a fundamental human right: *International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights*, 41st International Conference of Data Protection And Privacy Commissioners (21-24 October 2019, Tirana, Albania), online: < icdppc.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf > . Mass surveillance and the resulting loss of privacy and anonymity will effectively mean the loss of basic human rights such as freedom of speech or freedom of movement: Sharon Naker & Dov Greenbaum, "Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy" (2017) 23 B.U. J. Sci. & Tech. L. 88 at 101. However, international awareness and efforts regarding this technology is currently more focused on the public sector uses: Ewen MacAskill, "UN Report Criticises Use Of Facial Recognition By Welsh Police" *The Guardian* (29 June 2018), online: < www.theguardian.com/world/2018/jun/29/un-privacy-chief-criticises-use-of-facial-recognition-in-wales > ; Cynthia M. Wong, "We Underestimate the Threat of Facial Recognition Technology at Our Peril" *Human Rights Watch* (17 August 2018), online: < www.hrw.org/news/2018/08/17/we-underestimate-threat-facial-recognition-technology-our-peril > . The United Nations Human Rights Commission has released reports regarding mass surveillance of public by governments, where facial recognition tools have been classified under "obstacles to privacy": UNOHCHR, *Report of the Special Rapporteur on the right to privacy*, 23rd Sess., 2018, online: < www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_62_EN.docx > .

Microsoft president Brad Smith wrote on the company blog calling for regulation and warning that if unaddressed, soon the challenges that the technology brings "will be much more difficult to bottle back up."[128] The company has also rejected California law enforcement agency's request to install facial recognition technology on police cars and body cameras, stating that "it would lead to innocent women and minorities being disproportionately held for questioning because the artificial intelligence has been trained on mostly white and male pictures."[129] Microsoft's approach shows that regulation is urgently needed and jurisdictions cannot leave the regulation of the technology to market forces or self-regulation.[130]

In this section, first, the regulatory protections in jurisdictions outside of Canada will be examined in order to provide context for the proposed regulatory changes that are expressed in this paper. Later, amendments to PIPEDA will be proposed and a new provincial regulatory scheme will be addressed, respectively.

3.1 An Examination of Foreign Regulations

3.1.1 United States of America (U.S.)

Three states in the U.S. have enacted biometric data protection laws: Illinois,[131] Texas,[132] and Washington State.[133] Although it has a much broader

---

[128] Brad Smith, "Facial Recognition: It's Time for Action" *Microsoft on the Issues* (6 December 2018), online: < blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ > . The company is backing a bill that is not "too restrictive" and is opposing another proposed bill in Washington State: Tom Simonite, "Microsoft Wants Rules For Facial Recognition—Just Not These" *Wired* (21 February 2019), online: < www.wired.com/story/microsoft-wants-rules-facial-recognition-just-not-these/ > .

[129] Joseph Menn, "Microsoft Turned Down Facial-Recognition Sales On Human Rights Concerns" *Reuters* (16 April 2019), online: < www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV > . Axon, a major supplier of police body cameras and software, announced that it will not include facial recognition technology in its police body cameras after the company's AI ethics board concluded that facial recognition technology "is not reliable enough to justify its use in body cameras" and that there is "evidence of unequal and unreliable performance across races, ethnicities, genders and other identity groups": Christine Fisher, "Axon Won't Use Facial Recognition Tech in Its Police Body Cameras" *Engadget* (27 June 2019), online: < www.engadget.com/2019/06/27/axon-facial-recognition-ai-police-body-cameras > .

[130] The position of Microsoft in asking for regulation of the technology is important, however, it is also stated that the calls for regulation by Microsoft, Amazon and others make the debate about how the technology should be adopted, rather than *if* it should be adopted or not: Sidney Fussell, "The Strange Politics of Facial Recognition" *The Atlantic* (28 June 2019), online: < www.theatlantic.com/technology/archive/2019/06/democrats-and-republicans-passing-soft-regulations/592558 > .

[131] *Biometric Information Privacy Act*, 740 ILCS 14 (2007) [*BIPA*].

[132] Tex. Bus. & Com. Code § 503 [*Tex. Bus. & Com*].

scope, *The California Consumer Privacy Act* (CCPA),[134] which came into force on January 1, 2020, defines biometric information to include face prints.[135] The CCPA is an important statute that has strict data protection provisions, however it does not contain any additional precautions for facial recognition data or biometrics in general. In a recent effort, a federal bill regulating the commercial uses of facial recognition technologies has been proposed.[136]

Illinois' *Biometric Information Privacy Act* (BIPA) has been called "the gold standard for biometric protection"[137] and has been influential in raising awareness and the need for strong regulations for highly sensitive information. Therefore, it is important to examine BIPA in considering a new regulation for facial recognition technologies. BIPA came into force in 2008 and was the pioneer in regulation of biometric information in the U.S. However, perhaps BIPA's most significant provision is the right of action provided to individuals.[138] The inclusion of a private right of action has drawn attention to the regulation, creating awareness and generating a body of case law.

In 2016, an individual accused Shutterfly of using his face pattern to recognize and identify him in photographs posted to the platform, of which he was not a member.[139] The plaintiff had never used Shutterfly's services and had

---

[133] Wash. Rev. Code Ann. § 19.375 (2017). Washington State's law does not explicitly mention face prints amongst biometric identifiers. Curiously, the State also passed a public sector biometrics regulation on the same day with the private sector legislation, which includes the term "face geometry" amongst biometric identifiers: Wash. Rev. Code Ann. § 40.26.020 (2017). Furthermore, in May 2019 the city of San Francisco became the first city to ban the use of the technology by the public sector: Dave Lee, "San Francisco is the First US City to Ban Facial Recognition" *BBC* (15 May 2019), online: < www.bbc.com/news/technology-48276660 > . On October 2019, the state of California has passed legislation barring police from installing facial recognition technology on body-worn cameras for three years: Dustin Gardiner, "California Blocks Police from Using Facial Recognition in Body Cameras" *San Francisco Chronicle* (8 October 2019), online: < www.sfchronicle.com/politics/article/California-blocks-police-from-using-facial-14502547.php > .

[134] *The California Consumer Privacy Act of 2018*, 3 CIV § 1798. [*CCPA*].

[135] *Ibid* at § 1798.140.

[136] U.S. Bill S 847, *Commercial Facial Recognition Privacy Act of 2019*, 116th Cong, 2019; Makena Kelly, "New Facial Recognition Bill Would Require Consent Before Companies Could Share Data" *The Verge* (14 March 2019), online: < www.theverge.-com/2019/3/14/18266249/facial-recognition-bill-data-share-consent-senate-commercial-facial-recognition-privacy-act > . There is also a federal proposal in the U.S. that proposes to ban facial recognition and other biometric technologies in public housing units: U.S. Bill HR 4008, *No Biometric Barriers to Housing Act of 2019*, 116th Cong., 2019.

[137] Adam Schwartz, "New Attack on the Illinois Biometric Privacy Act" *Electronic Frontier Foundation* (10 April 2018), online: < www.eff.org/deeplinks/2018/04/new-attack-illinois-biometric-privacy-act > .

[138] *BIPA, supra* note 131 at §20. Texas regulation provides a civil penalty of a maximum $25.000 per violation that can be brought into action by the attorney general. *Tex. Bus. & Com, supra* note 132 at s. 503.001 (d).

never consented to the use of his facial data.[140] The District Court of Illinois first rejected Shutterfly's claim regarding jurisdiction, asserting that for a "private Illinois resident there is a strong interest in adjudicating the matter locally."[141] The Court then found that the use of facial recognition data without notice or consent was in violation of BIPA and found that the plaintiff had stated a claim to relief under BIPA.[142] However, in *McColough v. Smarte Carte Inc.*,[143] the Court for the Northern District of Illinois found that the plaintiff, whose fingerprints were scanned to provide secure access to public lockers, was not able to "show that she has statutory standing as a person "aggrieved by a violation" of BIPA."[144] In rejecting the plaintiff's claim, the Court examined §20 of BIPA, which states that "any person aggrieved by a violation of this Act shall have a right of action" and determined that an aggrieved person as described by the law needs to prove "an actual injury." This decision presented a dangerous precedent that was in contrast with the purpose of BIPA, which is to prevent businesses from collecting biometric information surreptitiously and recklessly. However, in a recent verdict, The Supreme Court of Illinois had the chance to examine who "an aggrieved person" under BIPA is. In this case, Six Flags amusement park's fingerprint collection for issuing monthly passes to the park was challenged.[145] The plaintiff, who was a minor and was represented by his mother, was required to give his fingerprints without any prior notice or consent from him or his legal guardian. The defendant alleged that the plaintiff did not suffer any actual injuries and thus did not have authority to sue under BIPA. Therefore, the question before the Court was "whether one qualifies as an "aggrieved" person and may seek liquidated damages and injunctive relief pursuant to the Act if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute."[146] The Court decided that the collection of biometric data without consent and the lack of policies regarding the uses and retention of the biometric data were violations of BIPA and no additional consequences needed to be proved. The Court stated in clear terms that "[t]he violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."[147] This verdict by the Supreme Court of Illinois can play a crucial part in a legal battle against Google's facial recognition technology,

---

[139] *Norberg v. Shutterfly Inc.*, 152 F.Supp.3d 1103 (N.D. Ill., Div. Eastern, 2015) [*Norberg v. Shutterfly*].

[140] *Ibid* at para. 7.

[141] *Ibid* at para. 5.

[142] *Ibid* at para. 7.

[143] *McColough v. Smarte Carte Inc.,* 2016 WL 4077108 (N.D. Ill., 2016) [*McColough v. Smarte Carte*].

[144] *Ibid* at para. 4.

[145] *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 (Ill., 2019) [*Rosenbach v. Six Flags*].

[146] *Ibid* at para. 1.

[147] *Ibid at* para. 33.

where the plaintiff's claim was rejected by the District Court for the same grounds.[148]

A recent settlement has once again demonstrated the effectiveness of BIPA in protecting the privacy of the residents of Illinois. Facebook's Tag Suggestions were the subject of a 2015 lawsuit which was later certified as a class-action.[149] The Court rejected Facebook's claims regarding applicable jurisdiction and the existence of actual harm, allowing the class-action suit to go forward.[150] Facebook's attempt to appeal the case at the Supreme Court, claiming that the class-action case should not be allowed to proceed because the group of users have not proven that they suffered an actual harm, was also denied.[151] A week later, Facebook announced that they agreed to pay $550 million to settle the class-action lawsuit.[152]

3.1.2 Europe (EU)

EU's General Data Protection Regulation[153] (GDPR) came into force on May 25, 2018. GDPR expanded the scope of the Directive[154] to provide union-wide rules that are more clear, certain and trustworthy.[155] Facial recognition data or biometrics in general were not specifically regulated in the Directive, but are explicitly regulated in the GDPR. Article 9 of the GDPR specifically prohibits processing of "special categories of personal data" which includes face templates.[156] Special category data are subject to stricter rules and can only be processed with explicit consent or with the limited exceptions provided in the article,[157] therefore banning the use of the technology in circumstances where the individual can be deemed to give implicit consent by being present in an area where the technology is deployed. GDPR requires an informed and

---

[148] Wendy Davis, "Google Takes Battle Over Biometrics To Appeals Court" *Media Post* (1 March 2019), online: < www.mediapost.com/publications/article/332648/google-takes-battle-over-biometrics-to-appeals-cou.html > .

[149] In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535 (N.D. Cal., 2018) at 540.

[150] *Ibid.*

[151] Emily Birnbaum, "Supreme Court Declines to Hear Facebook Facial Recognition Case" *The Hill* (21 January 2020), online: < thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case > .

[152] Natasha Singer & Mike Isaac, "Facebook to Pay $550 Million to Settle Facial Recognition Suit" *The New York Times* (29 January 2020), online: < www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html > .

[153] *General Data Protection Regulation*, Regulation 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, [2016] OJ L 119 [*GDPR*].

[154] *Directive, supra* note 88.

[155] Klein & Feuer, *supra* note 116 at 157.

[156] *GDPR, supra* note 153 at art. 4(14) defines "facial images" as part of biometric data.

[157] *GDPR*, *supra* note 153 at 9(2).

unambiguous consent that is given freely with a clear affirmative action.[158] Therefore, an individual has to be informed of the application prior to the processing of the data and accordingly signs in a mall advising of the use of the technology will not be enough to comply with GDPR.[159] GDPR also gives member countries the authority to introduce further limitations and conditions regarding to the processing of biometric data.[160]

Consequences of non-compliance with GDPR can be expensive. Organizations that breach GDPR can face penalties up to 4% of their annual global turnover or €20 million — whichever is greater.[161] The significant fines under GDPR could potentially have a more deterrent effect on the companies.[162] There are already many complaints against technology giants such as Facebook, Amazon, Netflix and YouTube, and Google was recently fined €50 Million by the French Data Protection Agency, CNIL for multiple violations.[163]

---

[158] Taylor Wessing & Debbie Heywood, "Facial Recognition Technology In The EU: Does GDPR Spell The End" *Lexology* (2 July 2018), online: < www.lexology.com/library/detail.aspx?g = 104d7d1d-80c4-4674-9286-b3a9ca7ee181 > .

[159] *Ibid.*

[160] *GDPR, supra* note 153 at 9(4).

[161] *Ibid* at art. 83. The U.K. fined Facebook £500,000 after the Cambridge Analytica scandal. The breach occurred before the GDPR was in force and this was the maximum fine under the Directive that could have been imposed at the time. U.K. Information Commissioner Elizabeth Denham stated that "[w]e considered these contraventions to be so serious we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR": Jim Waterson, "UK Fines Facebook £500,000 For Failing To Protect User Data" *The Guardian* (25 October 2018), online: < www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica > .

[162] However, considering the fact that the record fine of $5 billion by the U.S. F.T.C. laid on Facebook was considered "a win" for the company, which had a revenue of $15 billion in the first quarter of 2019, even the GDPR-scale fines will not be significant enough for big tech companies such as Facebook, Google or Amazon. Nilay Patel, "Facebook's $5 Billion FTC Fine Is an Embarrassing Joke" *The Verge* (12 July 2019), online: < www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke > .

[163] The Austria-based non-profit organisation "none of your business (noyb)" led by data activist Max Schrems has been active in filing complaints against tech companies with the introduction of GDPR. The organisation filed complaints against Facebook and Google the day that GDPR came into force: Noyb, "GDPR: noyb.eu Filed Four Complaints over "Forced Consent" Against Google, Instagram, Whatsapp and Facebook" (25 May 2018), online: . The organisation's complaint against Google resulted in a €50 million fine: CNIL, "The CNIL's Restricted Committee Imposes A Financial Penalty Of 50 Million Euros Against Google LLC" (21 January 2019), online: < www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc > . The organisation has also filed 8 other complaints to tech giants including Amazon, Netflix and YouTube: noyb, "Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access""(18 January 2019), online: .

3.2 Amending PIPEDA to Better Protect Canadians

Having established the shortcomings of the federal private sector privacy legislation PIPEDA in addressing the concerns that facial recognition technology brings, and the need for regulatory measures to be taken, this paper argues that the Act should be amended with provisions that are specific to facial recognition technologies. However, as will be further detailed below, amending PIPEDA alone will not solve the shortcomings of the Act.

3.2.1 Proposed Amendments to PIPEDA

The shortcomings of PIPEDA in addressing the privacy concerns raised by the use of facial recognition technologies have already been addressed.[164] Accordingly, the following amendments are proposed to PIPEDA in order to better protect Canadians from the private sector uses of facial recognition technology:

1. Sensitive Personal Information: A definition of sensitive personal information should be added to subsection 2(1) of PIPEDA, that specifically includes face templates or images and ideally also include any other types of biometric information, health information and financial information.
2. Collection, Use, Disclosure and Retention: It should be added to section 7 of PIPEDA that processing sensitive information as defined in the Act is prohibited, unless explicit consent is given by the data subject. Businesses should be prohibited from the use of facial templates for secondary purposes, even if data subjects consent to such use. Businesses should be required to permanently destroy collected sensitive information when the purpose of the collection has been satisfied or within 6 months of the last interaction of the data subject with the business.
3. Consent: PIPEDA's section 6.1 and the principle 4.3 of Schedule 1 should be amended to state that any interaction with sensitive information requires the explicit consent of the data subject and businesses are prohibited to rely on or accept implied consent for collecting, using or disclosing sensitive personal information. Businesses cannot seek the explicit consent of the data subject for the collection of sensitive information as a condition of service when their primary identified purpose does not require the use of it. In any written form or authorization, businesses have to provide an opt-in system where the data subject is initially opted-out of the collection of this data.
4. Safeguarding: It should be added to principle 4.7.2 of Schedule 1 that any interactions with sensitive information have to be electronically logged and recorded. It should be added to section 12.1 of PIPEDA that the Commissioner will audit the adequacy of the safeguards every 6 months and can perform random audits at their discretion.
5. Oversight and Enforcement: Sections 12 through 16 should be amended to provide the Commissioner with the powers to make binding orders and with

[164] See part 2, above.

the ability to issue monetary fines as well as mandate the application of certain practices.

6. Right of Action: A right of action should be introduced to PIPEDA, similar to BIPA.[165] BIPA's current provision awards damages of $1,000 for negligent violations and $5,000 for intentional violations per violation. The awards should be higher and more deterrent in PIPEDA, especially for big technology companies. After all, 100 intentional violations assessed by a court at a sum of $500,000 may be devastating for some small businesses but will not have the same effect for bigger players such as Google or Facebook. Therefore, a GDPR-like provision[166] where a certain percentage of revenues are accepted as damages, along with a set minimum fine, will be optimal. Furthermore, BIPA's lack of definition of an "aggrieved party" has led to confusion and some verdicts that were not favourable.[167] The legislation should specifically define that any person whose rights under this legislation are violated shall have a right of action without the need for proving any actual harm or injury.

3.2.2 PIPEDA's Limited Scope and the Act's Constitutional Challenges

One of the significant shortcomings of the Act when it comes to facial recognition is its inability to govern the use of these technologies in employment across all sectors.[168] Due to PIPEDA's somewhat delicate constitutional status, this aspect of the Act cannot be amended to provide protection for every Canadian worker. In other words, broadening the scope of the Act to cover the use of the technology by every private organization is impossible due to jurisdictional and constitutional challenges.

A short time following PIPEDA's enactment Quebec issued a decree indicating its intention to challenge PIPEDA's constitutionality in court.[169] The basis of the argument was that the federal government did not have the authority

---

[165] A private right of action was included in CASL, which was scheduled to come into force on July 1, 2017, however the government announced that the private right of action provisions of CASL were suspended. The government stated that "Canadian businesses, charities and non-profit groups should not have to bear the burden of unnecessary red tape and costs to comply with the legislation": Innovation, Science and Economic Development Canada, "Government of Canada Suspends Lawsuit Provision in Anti-Spam Legislation" (News release dated 7 June 2017), online: <www.canada.ca/en/innovation-science-economic-development/news/2017/06/government_of_canadasuspendslawsuitprovisioninanti-spamlegislati.html>. However, considering the significantly higher risk posed to individuals as opposed to spam, a similar approach would not be appropriate for facial recognition technologies.

[166] *GDPR, supra* note 153.

[167] *McColough v. Smarte Carte, supra* note 143.

[168] See part 2.3, above.

[169] Gouvernement du Québec, 17 December 2003, Decret No 1368-2003. Teresa Scassa & Michael Deturbide, *Electronic Commerce and Internet Law in Canada*, 2d ed (Toronto: CCH Canadian, 2012) at 92.

to regulate privacy, which falls under provincial jurisdiction according to the *Constitution Act*.[170] According to the *Constitution Act*, regulating "property and civil rights" of its citizens is in the jurisdiction of provinces.[171] The federal government, on the other hand, argued that it has the power to regulate "trade and commerce" [172] and thus PIPEDA falls under federal jurisdiction, as the Act specifically applies to commercial activities.[173] The criticisms of PIPEDA's constitutionality have been subdued. However, any attempt to broaden PIPEDA's scope beyond federally regulated employees will flare up the debates and constitutional challenges to the Act, as the federal government cannot regulate beyond "commercial activities" and employees of federal works or undertakings. Therefore, attempting to amend PIPEDA in order to give broader protections to employees from the dangers of facial recognition technology will not be successful and as a result, only amending PIPEDA in the other aspects discussed above, will not be sufficient in achieving the desired and necessary outcome.

3.3 Proposed Provincial Legislation

The limited scope of PIPEDA cannot be broadened by amending the Act, and accordingly, in order to protect every Canadian from the surreptitious uses of facial recognition technologies, provinces should enact specific laws protecting their residents. Regulation of privacy is no doubt in the provinces' jurisdiction in accordance with the *Constitution Act*.[174]

A provincial regulatory scheme that co-exists with PIPEDA to better protect privacy has precedent in Canada: the health information privacy laws. Health is accepted to be a matter of provincial jurisdiction[175] and therefore, privacy

---

[170] *Constitution Act*, *1867* (U.K.), 30 & 31 Vict, c. 3, s. 91, reprinted in R.S.C. 1985, App. II, No. 5 [*Constitution Act*].

[171] *Ibid* at s. 92(13).

[172] *Ibid* at s. 91(2).

[173] The federal government has also argued that personal information has a monetary value and has "become a tradable commodity": Michael Bastarache, "The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada's Reference re Securities Act" (June 2012) at 6, online: < accessprivacy.s3.amazonaws.-com/M-Bastarache-June-2012-Constitutionality-PIPEDA-Paper-2.pdf > . PIPEDA has been enacted in response to the EU's Data Protection Directive, to ensure data flow across the Atlantic. Therefore, holding PIPEDA *ultra vires* can have important international ramifications, especially concerning data flow with the EU and can have an effect on e-commerce: Josh Nisker, "PIPEDA: A Constitutional Analysis" (2007) 85 Can Bar Rev 317 at 318.

[174] *Constitution Act*, *supra* note 170. It should be noted that Alberta, British Columbia and Quebec have provincial private sector privacy laws that have been declared to be substantially similar. Accordingly, provincial workers in these provinces are protected under their respective legislations.

[175] Adrian Thorogood et al., "Protecting the Privacy of Canadians' Health Information in the Cloud" (2016), 14 CJLT 173 at 183.

protection in the health services context has been regulated provincially in Canada.[176] Several provinces have statutes that have been declared to be substantially similar to PIPEDA are exempt from it in matters relating to the scope of the provincial health information protection act.[177] In provinces with provincial health information protection acts that have not been yet declared to be substantially similar, PIPEDA and the provincial statutes are both in force. The same approach, where provinces enact privacy protections specifically for facial recognition technologies (or biometric technologies in general) would enable protection for all residents of the province and could co-exist with PIPEDA.

Provincial laws should include the principles outlined for the amendments to PIPEDA,[178] where facial templates would be specifically addressed. The statutes should demand businesses to acquire explicit, opt-in consent. Businesses should be prohibited from asking for the collection of this data unless their primary purpose clearly requires it and uses are documented in the written policies. The statutes should limit the collection, use, disclosure and retention of this data, ban the use of this data for secondary purposes and limit retention periods to 6 months. The provincial privacy commissioners could enforce the Acts and they would have significant investigation and enforcement powers. Such laws should also include a private right of action to residents with significant monetary awards. The laws should feature all of the provisions of the proposed amendments to PIPEDA, with a scope that would include any and all private sector uses of the technology.

The proposed provincial approach also has its downsides. Although the main principles should be adopted by each province, some differences might lead to a lack of uniformity amongst different provinces. PIPEDA's amended principles would be stronger in providing protection and accordingly, an acceptable uniform standard should be established throughout Canada. Furthermore, enacting provincial laws will bring significant costs to provinces. Public

---

[176] From 1997 to date, all of the common law provinces and territories of Canada, with the exception of Nunavut, have enacted provincial health information protection laws. Nunavut has neither a provincial health information protection act nor a private sector privacy act, therefore PIPEDA is applicable. Quebec's private sector privacy protection act, *An Act Respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1, is applicable in health information protection and is substantially similar to PIPEDA, therefore health information is regulated by the private sector act.

[177] Ontario's *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A, New Brunswick's *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05, Newfoundland and Labrador's *Personal Health Information Act*, S.N.L. 2008, c. P-7.01, and Nova Scotia's *Personal Health Information Act*, S.N.S. 2010, c. 41 were declared substantially similar to PIPEDA. These provinces are exempt from PIPEDA in health privacy matters, however PIPEDA may still be applicable in certain situations where personal health information travels across provincial or national borders: Adrian Thorogood et al., *supra* note 175.

[178] See part 3.2.1, above.

consultations, awareness campaigns and educational sessions for each province and territory will accumulate a high economic burden. However, this paper argues that regulating the uses of facial recognition technology and protecting individuals from its malicious uses is crucial in protecting the privacy and autonomy of Canadians, and similar to the health information protection legislations,[179] this dual approach is justified.

CONCLUSION

Facial recognition is a privacy threatening and highly intrusive technology, which is being widely used in commercial contexts, especially within consumer products. This paper argues that facial recognition technology is amongst one of the most invasive technologies, and that facial recognition data poses an even higher risk than other forms of biometric information. The nature of the advanced facial recognition technology tools allow the technology to be used on public surreptitiously, thus eliminating any form of notice and consent. It is almost impossible for one to hide their face in public and evade the technology, while being a member of society. There are structured databases in the hands of both public and private entities that are being used to identify individuals. Thus, the breach or misuse of this highly sensitive information brings major concerns of privacy, loss of anonymity and threats of fraud and identity theft.

In order to protect Canadians from this intrusive technology a dual approach is needed. First, PIPEDA should be amended in a significant way. Facial recognition data should be classified as sensitive data and be better protected accordingly. Businesses should be banned from collecting this information unless explicit consent is given by the data subject. PIPEDA's principles on collection, use, disclosure and retention should also be stricter for facial recognition data, where businesses are banned from using the data for secondary purposes and permanently delete the information within 6 months or when the purpose of collection is achieved. The OPCC should be given order-making powers, along with the ability to issue substantial monetary penalties. Lastly, a private right of action for individuals should be included in the Act.

Another significant shortcoming of PIPEDA is its limited scope. Accordingly, this paper proposes provincial acts to be enacted as well. Provincial protection acts will contain the amended principles of PIPEDA and will protect every resident in their jurisdictions. Although this dual approach has significant costs, this paper argues that the proposed regulatory scheme is required in order to protect every Canadian from the unregulated uses of technology and considering the dangers the technology poses on the privacy and autonomy of Canadians, these costs are justified.

---

[179] Given the importance placed on the privacy of very sensitive personal health information, every common law province and territory, with the exception of Nunavut, has enacted health information protection laws.

Along with the proposed amendments and new provincial laws, educating individuals on the dangers of this technology is equally important. If individuals are better informed of the actual threats this or any other future technology poses, then they can start to question these technologies and ask themselves which trade-offs are acceptable. Society needs to break the cycle that Winner has identified in 1986[180] and start demanding technology that is addressed to people's needs, not the other way around.

[180] Winner, *supra* note 15.