CANADA

PROVINCE DE QUÉBEC
DISTRICT DE **MONTRÉAL**

Nº : 500-09-029982-220

Nº : 500-06-001123-211

COUR D'APPEL

MICHAEL HOMSY, domicilié et résidant au [redacted]

APPELANT- Demandeur

c.

GOOGLE LLC, une personne morale dûment constituée ayant son siège au 1600, Amphitheatre Parkway, dans la ville de Mountain View, dans l'état de la Californie, 94043, États-Unis.

INTIMÉE - Défenderesse

DÉCLARATION D'APPEL
(article 352 *C.p.c.*)
Partie appelante
Datée du 28 mars 2022

AUX HONORABLES JUGES DE LA COUR D'APPEL DU QUÉBEC SIÉGEANT DANS LE DISTRICT D'APPEL DE MONTRÉAL, L'APPELANT EXPOSE RESPECTUEUSEMENT CE QUI SUIT :

I. INTRODUCTION

1. Le 1er mars 2022, l'Honorable Donald Bisson J.C.S. (le « **Juge** »), a rendu un jugement (le « **Jugement** », **Annexe 1**) qui a rejeté la *Originating application for authorization to institute a class action and to obtain the status of representative* (la « **Demande** », **Annexe 2**) de l'Appelant Michael Homsy (l'« **Appelant** ») qui tentait d'obtenir l'autorisation du Tribunal pour intenter une action collective en dommages et intérêts contre l'intimée Google LLC (l'« **Intimée** ») à la suite de l'extraction, la collecte, la conservation et/ou l'utilisation des données biométriques faciales à partir des photos téléchargées par les utilisateurs de *Google Photos*, et ce, sans avoir obtenu un

consentement préalable explicite;

2. Le Jugement comporte des erreurs de droit déterminantes desquelles découle une appréciation manifestement non fondée du critère de l'apparence de droit de l'article 575 (2) du Code de procédure civile;

3. Ces erreurs de droit ont amené le Juge à conclure, à tort, que l'Appelant n'avait pas rencontré le critère de l'article 575 (2) du *Code de procédure civile*, soit la démonstration d'une apparence de droit ou encore d'une cause défendable;

4. La présente *Déclaration d'appel* est déposée de plein droit par l'Appelant conformément à l'article 578 du *Code de procédure civile.* De plus, elle est déposée dans le délai d'appel de l'Appelant, lequel expirera le 4 avril 2022, l'avis de jugement étant daté du 3 mars 2022;

II. CONTEXTE

5. Le 28 octobre 2020, le commissaire à la protection de la vie privée du Canada, la commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique ont collectivement déposé un rapport traitant de la légalité de la collecte et de l'utilisation, par La Corporation Cadillac Fairview Limitée, d'une technologie d'analyse vidéo anonyme (l'**« AVA** »), laquelle utilisait un logiciel de reconnaissance faciale pour convertir des images en représentations numériques biométriques du visage des personnes qui visitaient ses centres commerciaux (le « **Rapport** », Pièce P-3, **Annexe 3**);

6. Il appert du Rapport que l'AVA utilise pour convertir les images en représentations numériques biométriques du visage des personnes un logiciel de « Reconnaissance Faciale » appelé FaceNet (« **FaceNet** »);

7. De plus, le Rapport réfère à une publication scientifique datée du 17 juin 2015 qui indique que FaceNet est une technologie de reconnaissance faciale qui a été développée par trois des ingénieurs de l'Intimée (la « **Publication scientifique** »,

Pièce P-8, **Annexe 4**);

8. Le Rapport conclut que l'utilisation de FaceNet pour convertir les images en représentations numériques biométriques du visage des personnes constitue une collecte de renseignements biométriques susceptible de permettre la reconnaissance de personnes spécifiques, le tout tel qu'il appert du paragraphe 65 du Rapport;

9. Le Rapport conclut également que l'utilisation de FaceNet pour convertir les images en représentations numériques biométriques du visage des personnes nécessite l'obtention d'un consentement explicite, le tout tel qu'il appert du paragraphe 81 du Rapport;

10. L'Appelant soutient dans sa Demande que, depuis le 28 octobre 2015, l'Intimée a utilisé FaceNet au Canada afin de convertir les visages présents sur les photos téléchargées par ses utilisateurs vers sa plateforme *Google Photos* en représentations numériques biométriques, et ce, sans que l'Intimée ait obtenu au préalable un consentement explicite de ses utilisateurs, le tout tel qu'il appert d'un article annonçant l'intégration de la technologie de reconnaissance faciale dans *Google Photos* au Canada (l'« **Article** », Pièce P-5, **Annexe 5**);

11. Ainsi, l'Appelant soutient que l'Intimée a illégalement extrait, collecté, conservé et/ou utilisé les données biométriques faciales des personnes dont le visage apparaissait sur des photos téléchargées vers sa plateforme *Google Photos*;

12. D'ailleurs, l'Intimée a avoué dans un acte de procédure produit au dossier, soit l'*Application for authorization to adduce relevant evidence and to examine the applicant* (l'« **Acte de procédure** », **Annexe 6**), que FaceNet était « Google's Algorithm which processes images of faces » et que *Google Photos* offrait un « face grouping feature »;

13. L'Appelant soutient dans sa Demande que cette pratique de l'Intimée porte sciemment atteinte aux droits à la vie privée et à l'inviolabilité des membres protégés par la *Charte des droits et libertés de la personne*;

14. De plus, l'Appelant soutient que l'Intimée a manqué aux obligations qui lui incombent en vertu du *Code civil du Québec* et de la *Loi sur la protection des renseignements personnels dans le secteur privé*;

15. Finalement, l'Appelant allègue que l'Intimée a fait des représentations trompeuses aux utilisateurs de *Google Photos*, et ce, en violation de la *Loi sur la protection du consommateur*;

16. L'Appelant, par l'action collective envisagée, recherche :

- La condamnation de l'Intimée au paiement de dommages moraux;
- La condamnation de l'Intimée au paiement de dommages matériels; et
- La condamnation de l'Intimée au paiement de dommages punitifs.

III. LE CRITÈRE DE L'ARTICLE 575 (2) DU CODE DE PROCÉDURE CIVILE EST RENCONTRÉ

17. Le Jugement comporte les erreurs de droit déterminantes suivantes :

(A) Le Juge a commis une erreur de droit en omettant de considérer les aveux judiciaires faits par l'Intimée dans son Acte de procédure soient :

a. Que FaceNet est l'algorithme de l'Intimée et qu'il est utilisé pour « process » les images de visages (**Annexe 6**, par. 14 d) ii.); et

b. Que *Google Photos* offre un « face grouping feature » (**Annexe 6**, par. 14 d) i.).

(B) Le Juge a commis une erreur de droit en adoptant une interprétation restrictive et littérale des allégations de la Demande et des éléments de preuve à son soutien, et ce, alors que l'état du droit impose une interprétation large et libérale qui permet l'analyse de la Demande comme « un tout » pour déterminer si les critères de l'article 575 du *Code de procédure civile* sont rencontrés;

(C) Le Juge a commis une erreur de droit en imposant à l'Appelant un fardeau de preuve alors que l'état du droit exige uniquement un fardeau de démonstration d'une cause défendable;

18. Ces erreurs de droit ont amené le Juge à avoir une appréciation manifestement non fondée des faits en cause. En effet, une appréciation correcte des faits en cause aurait permis au Juge de conclure que l'Appelant avait présenté une « certaine preuve » et qu'il devait donc tenir pour avérées les allégations de la Demande relativement à l'utilisation par l'Intimée du logiciel de reconnaissance faciale FaceNet pour procéder à l'extraction, la collecte, la conservation et/ou l'utilisation des données biométriques faciales des personnes dont le visage se retrouve sur les photos téléchargées par des utilisateurs sur sa plateforme *Google Photos*, et ce, sans avoir obtenu le consentement explicite desdites personnes;

19. Ainsi, c'est notamment en raison de cette appréciation manifestement non fondée des faits que le Juge a conclu qu'il n'y avait pas d'apparence de droit et que le critère prévu à l'article 575 (2) du *Code de procédure civile* n'était donc pas rencontré;

A. L'OMISSION DU JUGE DE CONSIDÉRER LES AVEUX JUDICIAIRES FAITS PAR L'INTIMÉE DANS UN ACTE DE PROCÉDURE QU'ELLE A PRODUIT AU DOSSIER CONSTITUE UNE ERREUR DE DROIT DÉTERMINANTE

20. Le Juge a refusé d'autoriser l'action collective envisagée au motif suivant :

> « *Le demandeur n'a donc pas démontré une cause défendable quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales par la défenderesse*. »

21. Le Juge en arrive à cette conclusion en soutenant que l'Appelant n'a pas présenté une « certaine preuve » permettant de soutenir l'allégation à l'effet que FaceNet est bien l'algorithme utilisé par l'Intimée dans *Google Photos* pour faire l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales;

22. Or, l'Intimée a admis dans l'Acte de procédure que :

> *« "Facenet" (Google's algorithm which processes images of faces) does not attempt to determine a person's identity from a photo; »*

23. De plus, l'Intimée a également admis dans l'Acte de procédure que :

« the Google Photos face grouping feature is optional and can be disabled by the user at any time; »

24. Ainsi, il ressort de ces admissions que FaceNet est l'algorithme de reconnaissance faciale de l'Intimée et que l'Intimée utilise FaceNet dans ses diverses plateformes, tel *Google Photos*, et ce, lorsqu'un traitement d'images de visages est requis;

25. Ces admissions constituent un aveu judiciaire fait par l'entremise des avocats de l'Intimée, au sens de l'article 2852 du *Code civil du Québec*;

26. En effet, l'Intimée, par l'entremise de ses avocats, a clairement et sans ambiguïté admis les éléments factuels ci-haut allégués;

27. En tenant compte de ces admissions, du Rapport et des autres éléments de preuve au dossier, il est évident que l'Appelant a présenté une « certaine preuve » permettant d'établir que l'Intimée a utilisé FaceNet pour faire l'extraction, la collecte, la conservation et l'utilisation de données biométriques faciales dans *Google Photos*;

28. Les avocats de l'Appelant ont plaidé ces admissions au Juge lors de l'audience du 21 février 2022, mais ce dernier les a écartées en mentionnant qu'un aveu judiciaire ne pouvait se retrouver dans un Acte de procédure préalablement rejeté. L'Appelant soumet respectueusement que le Juge a erré en droit en indiquant que les admissions de l'Intimée ne pouvaient être invoquées à titre d'aveu judiciaire au motif que l'Acte de procédure avait été rejeté et n'était donc plus au dossier;

29. En effet, il est reconnu tant en doctrine qu'en jurisprudence que l'aveu judiciaire d'une partie est toujours recevable, sauf exceptions qui ne trouvent pas application dans le présent dossier. De plus, l'article 2852 alinéa 1 du *Code civil du Québec* stipule clairement que l'aveu judiciaire ne peut être révoqué, sauf en cas d'erreur de faits;

30. Avec égards, l'Appelant soutient que le Juge a commis une erreur de droit en omettant de considérer les aveux de l'Intimée dans son analyse de l'existence d'une « certaine preuve » au soutien des allégations de la Demande;

31. Par conséquent, l'Appelant soumet respectueusement que n'eut été cette erreur de droit du Juge, il aurait rencontré la condition de l'article 575 (2) du *Code de procédure civile*, soit la démonstration d'une apparence de droit ou encore d'une cause défendable eut égard aux faits allégués dans la Demande;

B. L'INTERPRÉTATION RESTRICTIVE ET LITTÉRALE DES ALLÉGATIONS DE LA DEMANDE ET DES ÉLÉMENTS DE PREUVE À SON SOUTIEN CONSTITUE UNE ERREUR DE DROIT

32. Au paragraphe 12 du Jugement, le Juge rappelle les principes établis par la Cour Suprême du Canada relativement à l'article 575 du *Code de procédure civile,* notamment en matière d'interprétation restrictive et littérale :

> « *Les conditions de l'article 575 Cpc doivent être appliquées de manière souple, libérale et généreuse afin de faciliter l'exercice de l'action collective comme moyen d'atteindre le double objectif de la dissuasion et de l'indemnisation des victimes. Tout doute doit jouer en faveur de l'autorisation* ;
>
> *[…]*
>
> *Le Tribunal doit prêter une attention particulière, non seulement aux faits allégués, mais aussi aux inférences ou présomptions de fait ou de droit qui sont susceptibles d'en découler et qui peuvent servir à établir l'existence d'une « cause défendable ».* »
>
> **[nos soulignements]**

33. Par la suite, le Juge décrit la méthode utilisée pour vérifier si les critères de l'article 575 du *Code de procédure civile* sont remplis, comme suit :

> *« Le Tribunal étudie maintenant en détail tous les paragraphes pertinents de la Demande portant sur l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales par la défenderesse. Il s'agit d'analyser les paragraphes un par un, ou groupe par groupe, et ensuite si requis, de considérer leur effet cumulatif. »*
>
> **[nos soulignements]**

34. Le Jugement enchaîne ensuite avec l'analyse du Juge, allégation par allégation, puis groupe d'allégations par groupe d'allégations, du caractère avéré de celles-ci et, en l'absence d'un tel caractère, à vérifier si les allégations sont soutenues par une « certaine preuve »;

35. Enfin, le Juge conclut son analyse des critères de l'article 575 du *Code de procédure*

civile de la manière suivante :

> *« Le Tribunal conclut que, dans ces circonstances, que ce soit de façon individuelle ou même par leur effet cumulatif, les allégations du demandeur sur sa première allégation de pratique factuelle de la défenderesse ne peuvent être tenues pour avérées. »*
>
> **[nos soulignements]**

36. Or, dans les faits, suite à son analyse des allégations de la Demande paragraphe par paragraphe, puis groupe de paragraphes par groupe de paragraphes, le Juge a omis d'examiner lesdites allégations sous leur effet cumulatif, comme il l'avait pourtant établi dans sa méthode d'analyse;

37. Le Juge a donc commis une erreur de droit en concluant à l'absence du caractère avéré des allégations de la Demande et à l'absence d'une « certaine preuve » à son soutien, sans avoir préalablement analysé leur effet cumulatif;

38. En effet, l'état du droit en matière d'action collective impose une interprétation large et libérale qui permet au Tribunal d'analyser la Demande comme un tout pour déterminer si les critères de l'article 575 du *Code de procédure civile* sont rencontrés;

39. À titre d'exemple, reprenons certains éléments du Jugement relativement à l'analyse des allégations de la Demande et des éléments de preuve à son soutien :

- Publication scientifique
    - Le juge a écarté la Publication scientifique à titre de « certaine preuve », car, bien que trois ingénieurs de l'Intimée en soient les auteurs, il n'y est pas spécifiquement écrit que l'Intimée utilise le logiciel décrit, soit FaceNet;
- Rapport
    - Le Rapport est écarté par le Juge à titre de « certaine preuve », puisqu'il ne contient aucune référence directe à l'Intimée;
- Article

- Le Juge écarte l'Article à titre de « certaine preuve » puisqu'il juge que l'auteur et la source sont inconnus et invérifiables;

40. C'est cette analyse qui a mené le Juge à conclure qu'individuellement chacune des pièces ne pouvait constituer une « certaine preuve ». Or, le Juge a omis et/ou négligé d'analyser l'effet cumulatif des éléments de preuve mentionnés ci-haut. Ainsi, le Juge a adopté une approche restrictive, littérale et donc contraire à l'état du droit en vigueur;

41. Avec égards, le Juge a ainsi omis de porter une attention particulière aux inférences et aux présomptions de faits qui découlent des allégations de la Demande ainsi que des pièces à son soutien;

42. À cette fin, reprenons certains faits allégués dans la Demande :

- Le 17 juin 2015, trois ingénieurs de l'Intimée publient la Publication scientifique dans laquelle ils expliquent le fonctionnement de FaceNet, un logiciel de « Reconnaissance Faciale »;

- Le 28 octobre 2015, l'Article est publié sur un site web afin d'annoncer l'arrivée de *Google Photos* au Canada, indiquant par le fait même que la plateforme pourra « recognize faces and group them together »; et

- Le 28 octobre 2020, le Rapport est déposé par plusieurs commissaires et conclu que l'AVA utilise le logiciel de reconnaissance faciale FaceNet, technologie qui ne respecte pas la réglementation en matière de respect de la vie privée.

43. Ainsi, quoique les éléments de preuve au soutien de la Demande ne démontrent pas directement que FaceNet est implémenté dans *Google Photos,* la balance entre les faits connus et prouvés permettait par induction d'en venir à une telle conclusion au stade de l'autorisation d'une action collective où uniquement une « certaine preuve » est requise, soit un fardeau au seuil peu élevé;

44. Le Juge a donc erré en droit en adoptant une interprétation restrictive et littérale des allégations de la Demande et des éléments de preuve à son soutien. Par conséquent,

l'Appelant soumet qu'il a rencontré la condition de l'article 575 (2) du *Code de procédure civile*, soit la démonstration d'une apparence de droit ou encore d'une cause défendable;

C. IMPOSER À L'APPELANT UN FARDEAU DE PREUVE ALORS QUE L'ÉTAT DU DROIT EXIGE UNIQUEMENT UN FARDEAU DE DÉMONSTRATION D'UNE CAUSE DÉFENDABLE CONSTITUE UNE ERREUR DE DROIT

45. Au paragraphe 12 du Jugement, le Juge rappelle les principes établis par la Cour Suprême du Canada relativement à l'article 575 du *Code de procédure civile,* notamment quant au fardeau de preuve exigé au stade de l'autorisation d'une action collective :

> *« L'autorisation d'un recours collectif au Québec nécessite l'atteinte d'un seuil peu élevé ;*
>
> *[…]*
>
> *La vocation de l'étape de l'autorisation du recours collectif est d'exercer une fonction de filtrage pour écarter les demandes frivoles, sans plus. L'exercice auquel le Tribunal est convié en est un de filtrage dont l'objectif est de se satisfaire de l'existence d'une cause défendable.*
>
> *[...]*
>
> *Quant à l'apparence de droit, le requérant n'a qu'un fardeau de démonstration et non de preuve. Il doit démontrer l'existence d'une « apparence sérieuse de droit », d'une « cause défendable »; »*
>
> **[nos soulignements]**

46. Par la suite, le Juge a procédé à l'analyse du critère de l'apparence droit en examinant les allégations de la Demande et les éléments de preuve à leur soutien;

47. Or, cet examen démontre que le Juge a exigé, à plusieurs reprises, que l'Appelant remplisse un fardeau de preuve, alors qu'au stade de l'autorisation d'une action collective seul un fardeau de démonstration d'une cause défendable est nécessaire. Plus spécifiquement, le Juge a écarté trois éléments de preuve en indiquant que ceux-ci ne constituaient pas une « certaine preuve », exigeant par le fait même un fardeau plus élevé que celui de démontrer une cause défendable;

48. En premier lieu, le Juge a erronément écarté la Publication scientifique à titre de « certaine preuve »;

49. En effet, en produisant en preuve la Publication scientifique, soit un document qui explique le fonctionnement de FaceNet, lequel est signé par trois ingénieurs de l'Intimée et sur lequel figure les adresses courriel professionnelles de ceux-ci ainsi que le nom « Google Inc. », soit l'ancêtre de l'Intimée, l'Appelant soumet qu'il a rempli son fardeau de démontrer que le logiciel FaceNet a bel et bien été développé par cette dernière;

50. La Publication scientifique contient également 48 références au mot « our » pour décrire l'algorithme, la recherche effectuée et les méthodes utilisées;

51. Les auteurs ayant signé la Publication scientifique sous l'effigie de « Google Inc. », soit l'ancêtre de l'Intimée, le terme « our » fait alors autant référence aux auteurs individuels qu'à l'Intimée, soit leur employeur;

52. Or, le Juge a rejeté cet argument au motif suivant :

> *« Il s'agit d'une qualification par les auteurs de leur algorithme, leur recherche, leur méthode. Il ne s'agit aucunement d'une mention selon laquelle la défenderesse utiliserait ce logiciel dans Google Photos ni même ailleurs dans ses produits; »*

53. Avec égards, nous soumettons que le Juge erre ici en droit en exigeant non seulement de prouver que FaceNet a été développé par l'Intimée, mais également que ledit logiciel est utilisé dans les diverses plateformes de l'Intimée, notamment *Google Photos*;

54. Vu la nature immatérielle et secrète d'un algorithme tel FaceNet, il est en effet difficile, voire impossible, de démontrer une telle utilisation spécifique au stade de l'autorisation d'une action collective et, de ce fait, sans avoir eu l'opportunité d'interroger l'Intimée au préalable;

55. On retrouve également dans la publication une référence au terme « GoogLeNet » dans un paragraphe qui quoique technique vient minimalement créer un doute quant aux liens entre FaceNet et l'Intimée, doute qui doit d'ailleurs jouer en faveur de l'Appelant;

56. Le Juge soulève également que la Publication scientifique, publiée le 17 juin 2015, ne

peut constituer une « certaine preuve » puisqu'il ressort de celle-ci que FaceNet n'est pas encore fonctionnel et constitue plutôt une hypothèse de travail. Or, le Rapport déposé le 28 octobre 2020 indique clairement que FaceNet est utilisé de manière fonctionnelle dans les centres commerciaux appartenant à La Corporation Cadillac Fairview Limitée. Il est ainsi erroné de conclure que FaceNet n'a jamais été fonctionnel durant la « Class Period », soit depuis le 28 octobre 2015;

57. L'Appelant soumet donc qu'il ressort de cette analyse du Juge qu'un fardeau supérieur à celui de démonstration lui a été imposé;

58. En deuxième lieu, le Juge a erronément écarté le Rapport à titre de « certaine preuve », soit une pièce centrale au soutien des allégations de la Demande et de laquelle de nombreuses inférences et présomptions de faits auraient dû être tirées;

59. Or, le Juge a rejeté le Rapport pour le motif suivant :

> *« Or, les paragraphes 3 et 12 à 21 de la Demande et les Pièces P-2 à P-4 ne contiennent aucune référence à la défenderesse, ni de près, ni de loin, ni spécifiquement. Donc en soi, sans rien d'autre, selon le Tribunal, ils ne peuvent constituer une preuve permettant de venir supporter une allégation de fait visant la défenderesse ; »*

60. Le Juge a également écarté le Rapport puisque rien ne permettait de relier directement FaceNet à l'Intimée;

61. Or, en exigeant que le Rapport contienne une mention claire et non équivoque à l'Intimée, le Juge impose un fardeau de preuve plutôt qu'un fardeau de démonstration. Ce fardeau de preuve imposé à l'Appelant est trop élevé, puisque le Juge impose, à tort, à l'Appelant de prouver que l'Intimée utilise FaceNet dans *Google Photos*;

62. En troisième lieu, le Juge a erronément écarté l'Article à titre de « certaine preuve » sous le seul motif qu'il considère l'Article être l'opinion d'un auteur inconnu et invérifiable. Ainsi, le Juge reproche à l'Appelant de ne pas être en mesure de démontrer la crédibilité de l'auteur de l'Article et que ce manque de crédibilité l'empêche de considérer l'Article comme une « certaine preuve »;

63. Or, en exigeant de l'Appelant un profil complet de l'auteur de l'Article pour démontrer

qu'il s'agit d'un « vrai journaliste » et que l'Article constitue une « publication scientifique rigoureuse » et/ou « une enquête journalistique suffisante », le Juge exige de l'Appelant un fardeau qui va bien au-delà du simple fardeau de démonstration d'une apparence de droit ou d'une cause défendable;

64. Le Juge considère également que l'Article manque de détails :

> *« Par ailleurs, même en supposant qu'il soit valide comme « certaine preuve » - ce qu'il n'est pas - le texte de la Pièce P-5 est plutôt laconique et avare de détails spécifiques quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales. De l'avis du Tribunal, son absence de détail confirme qu'il s'agit de l'opinion personnelle de l'auteur ; »*

65. Toutefois, l'Article fait une référence directe à une version de *Google Photos* disponible aux États-Unis qui permet de « recognize faces and group them together » et qu'une version similaire serait bientôt disponible au Canada;

66. L'Appelant soumet respectueusement que le Juge a erré en exigeant de l'Appelant une preuve plutôt qu'une démonstration, et ce, en concluant que l'Article était une opinion de son auteur qui ne contient pas assez de « détails spécifiques quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales ». En exigeant une preuve aussi détaillée, spécifique et précise, il est évident que le Juge a exigé à l'Appelant un fardeau plus élevé que celui de simplement démontrer une apparence de droit ou une cause défendable. De plus, en cas de doute quant à la véracité des propos de l'Article, l'Appelant soumet que ce doute devrait jouer en sa faveur;

67. Enfin, le Juge conclut son analyse du critère de l'apparence de droit en employant les termes suivants :

> *« Autrement dit, puisque le demandeur n'a pas démontré l'existence de la pratique alléguée d'extraction, de collecte, de conservation et d'utilisation des données biométriques faciales, il est donc inutile de savoir si la défenderesse a fourni ou non de préavis suffisant ou a obtenu le consentement du demandeur et des membres du groupe ou leur a fait des fausses représentations. Également, pour les mêmes raisons, il ne peut y avoir de dommages punitifs. »*
>
> **[nos soulignements]**

68. Respectueusement, l'Appelant soumet que le Juge a erré en droit en indiquant que l'Appelant aurait dû démontrer « l'existence de la pratique alléguée d'extraction, de

collecte, de conservation et d'utilisation des données biométriques faciales »;

69. En effet, le fardeau de l'Appelant était plutôt de démontrer l'existence d'une cause défendable relativement à la pratique alléguée d'extraction, de collecte, de conservation et d'utilisation des données biométriques faciales;

70. Il faut donc en venir à la conclusion que le Juge a erré en droit en imposant à l'Appelant un fardeau de preuve plutôt qu'un fardeau de démonstration d'une apparence de droit ou d'une cause défendable;

71. Par conséquent, l'Appelant soumet avec égard que n'eut été cette erreur de droit du Juge, il aurait rencontré la condition de l'article 575 (2) du *Code de procédure civile*, soit la démonstration d'une apparence de droit ou encore d'une cause défendable;

72. L'intérêt de la justice requiert donc l'intervention de la Cour d'appel pour rectifier lesdites erreurs de droit;

73. La présente déclaration est bien fondée en faits et en droit;

PAR CES MOTIFS, PLAISE À LA COUR D'APPEL DE :

ALLOW the appeal;

SET ASIDE the first instance judgment rendered on March 1, 2022, by the Honourable Donald Bisson J.C.S. which dismisses the *Originating application for authorization to institute a class action and to obtain the status of representative*;

GRANT the « Appelant »'s *Originating application for authorization to institute a class action and to obtain the status or representative* against the « Intimée »;

AUTHORIZE the following Class action:

> ***An action in damages against the « Intimée » in reparation of the harm caused by the « Intimée »'s unlawful violation of the Class Member's right to privacy and inviolability, and its misrepresentations and omissions regarding the privacy features of its Google Photos application.***

GRANT the status of representative to Michael Homsy for the purpose of instituting the said Class action for the benefit of the following group of persons, namely:

> ***All individuals residing in the Province of Quebec, except for Excluded Persons, who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos during the Class Period.***

IDENTIFY the principal questions of law and of fact to be dealt with collectively as follows:

A. Did the « Intimée » breach articles 3,10, 35, 36, and/or 37, and 1457 and/or 1458 of the *Civil Code of Québec*?

B. Did the « Intimée » breach its statutory obligations under the *Act Respecting the Protection of Personal Information in the Private Sector*?

C. Did the « Intimée » breach articles 1 and/or 5 of the *Charter of Human Rights and Freedoms*?

D. Did the « Intimée » breach articles 219 and 228 of the *Consumer Protection Act*?

E. Are Class Members entitled to material and/or moral damages?

F. Are Class Members entitled to punitive damages?

G. What are the amounts of the aggregate moral, material and punitive damages to be awarded to the Class?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

a. **GRANT** the « Appelant »'s action against the « Intimée »;

b. **DECLARE** that the « Intimée »:

i. Violated its statutory obligations under the *Civil Code of Québec* and the

Act Respecting the Protection of Personal Information in the Private Sector;

ii. Intentionally and unlawfully violated class members' rights to privacy and inviolability under the *Charter of Human Rights and Freedoms*;

iii. Violated its statutory obligations under the *Consumer Protection Act*;

c. **CONDEMN** the « Intimée » to pay the Class Members material, moral and punitive damages in amounts to be determined by the Court based on the evidence at trial;

d. **ORDER** collective recovery in accordance with articles 595-598 of the *Code of Civil Procedure* for the moral and punitive damages, and individual recovery with articles 599-601 of the *Code of Civil Procedure* for the material damages;

e. **CONDEMN** the « Intimée » to any other remedy deemed appropriate, just, and reasonable;

THE WHOLE WITH COST, with legal costs, including the costs of all publications of notices, experts and expert reports and the attendance fees of the experts to present these reports in Court.

DECLARE that all Class Members that have not requested their exclusion from the Class in the prescribed delay to be bound by any judgment to be rendered on the class action to be instituted;

FIX the delay of exclusion at 30 days from the date of the publication of the notice to the Class Members;

ORDER the publication of a notice to the Class Members in accordance with article 579 of the *Code of Civil Procedure*, pursuant to a further Order of the Court of first instance;

REFER to the Court of first instance to determine the content of the notice to the Class Members in accordance with article 603 of the *Code of Civil Procedure*;

ORDER that the class action be tried in the judicial district of Montreal;

CONDEMN the « Intimée » to pay the « Appelant » legal costs both in first instance and on appeal.

TORONTO, ce 28e jour de mars 2022

Investigation Counsel P.C.

INVESTIGATION COUNSEL PC
Avocats de l'Appelant
Me John Archibald
jarchibald@investigationcounsel.com
350 Bay Street, Suite 300
Toronto, ON, M5H 2S6
Téléphone : 416 637 3152
Fax : 416 637 3445

MONTRÉAL, ce 28e jour de mars 2022

CaLex Légal inc.

CALEX LÉGAL INC.
Avocats de l'Appelant
Me Jean-Philippe Caron
Me Alessandra Esposito Chartrand
Me Gabriel Bois
Benjamin Tavernier-Labrie, stagiaire
jpc@calex.legal | aec@calex.legal
gb@calex.legal | btl@calex.legal
4214 rue St-Jacques
Montréal, QC, H4C 1J4
Téléphone : 514 548 3023
Fax : 514 846 8844
N/R : 1349-01
BP3268

Signature Certificate

Reference number: EDSE6-BAEAH-XLB9X-QZZA2

Signer	Timestamp	Signature
John Archibald Email: jarchibald@investigationcounsel.com		Investigation Counsel P.C.
Sent:	28 Mar 2022 17:30:21 UTC	
Viewed:	28 Mar 2022 17:30:38 UTC	IP address: 208.69.14.151
Signed:	28 Mar 2022 17:31:12 UTC	Location: Markham, Canada
Jean-Philippe Caron Email: jpc@calex.legal		CaLex Légal inc.
Sent:	28 Mar 2022 17:30:21 UTC	
Viewed:	28 Mar 2022 17:31:45 UTC	IP address: 50.100.114.228
Signed:	28 Mar 2022 17:32:32 UTC	Location: Montreal, Canada

Document completed by all parties on:
28 Mar 2022 17:32:32 UTC

ANNEXE 1

COUR SUPÉRIEURE

(Actions collectives)

CANADA
PROVINCE DE QUÉBEC
DISTRICT DE MONTREAL

N°: 500-06-001123-211

DATE: 1er mars 2022

SOUS LA PRÉSIDENCE DE: L'HONORABLE DONALD BISSON, J.S.C. (JB4644)

MICHAEL HOMSY
Demandeur

v.

GOOGLE LLC
Défenderesse

JUGEMENT

(sur demande d'autorisation d'exercer une action collective)

TABLE DES MATIÈRE

1. INTRODUCTION

[1] Le 15 janvier 2021, le demandeur Michael Homsy a déposé une *Originating Application for Authorization to Institute a Class Action and to Obtain the Status of Representative* (la « Demande ») aux termes de laquelle il demande au Tribunal l'autorisation d'exercer une action collective contre la défenderesse Google LLC et de se voir attribuer le statut de représentant pour le groupe proposé suivant :

> User Class: All individuals residing in the Province of Quebec, except for the Excluded Persons*, who used Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos since October 28th, 2015 (the "Class Period");
>
> Non-User Class: All individuals residing in the Province of Quebec, except for the Excluded Persons, who did not use Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos during the Class Period;
>
> *Excluded Persons" means Google and its parent corporations, subsidiaries, affiliates, predecessors, successors *and assigns; and their current or former officers, directors, and legal representatives*

[2] Le demandeur reproche à la défenderesse d'avoir procédé, *via* l'application Google Photos, à l'extraction, à la collecte, à la conservation et à l'utilisation des données biométriques faciales des résidents du Québec, sans fournir de préavis suffisant, sans obtenir un consentement éclairé et sans publier de politiques de conservation des données biométriques et ce, depuis octobre 2015. Selon le demandeur, les données biométriques faciales sont biologiquement uniques à chaque membre du groupe et donc de nature intrinsèquement privées et personnelles, comme les empreintes digitales et l'ADN[1].

[3] Le demandeur soutient que la défenderesse a agi illégalement et en portant sciemment atteinte aux droits à la vie privée et à l'inviolabilité des membres protégés par la *Charte des droits et libertés de la personne*[2] (la « Charte »). Il ajoute que la défenderesse a manqué aux obligations qui lui incombent en vertu du *Code civil du Québec* (« CcQ ») et de la *Loi sur la protection des renseignements personnels dans le secteur privé*[3] (la « LPRPSP »). Le demandeur soutient également que la défenderesse

---

1 Le demandeur fait référence à la Pièce P-2.
2 RLRQ c. C-12.
3 RLRQ c. P-39.1.

a fait des représentations trompeuses aux utilisateurs de Google Photos au sujet de ses pratiques et politiques de confidentialité, et ce, en violation de la *Loi sur la protection du consommateur*[4] (la « LPC »). Plus spécifiquement, le demandeur allègue que la défenderesse a omis et/ou négligé de décrire avec précision, voire d'informer le consommateur qu'elle procédait à l'extraction, la collecte, la conservation et l'utilisation de renseignements personnels sensibles sous forme de données biométriques faciales à partir des photos conservées sur sa plateforme Google Photos.

[4] L'action collective envisagée recherche : 1) une condamnation de la défenderesse au paiement de dommages moraux pour compenser les inconvénients et l'anxiété vécus par les membres du groupe; 2) une condamnation de la défenderesse au paiement de dommages matériels équivalant aux sommes dépensées par les membres du groupe à la suite de l'extraction de leurs données biométriques; et 3) l'attribution de dommages punitifs suffisants pour dissuader tant la défenderesse que d'autres sociétés technologiques de porter intentionnellement et illicitement atteinte au droit à l'intégrité de la personne des résidents du Québec ainsi qu'à leur droit au respect de leur vie privée.

[5] La défenderesse conteste et argumente que le demandeur n'a démontré aucune apparence de droit et qu'il n'a en conséquence aucun intérêt pour être un représentant valide. La défenderesse présente également des arguments subsidiaires sur la redéfinition du groupe[5] et la portée temporelle du groupe.

2. ANALYSE ET DISCUSSION

2.1 Dispositions législatives invoquées par le demandeur

[6] Voici les articles 1, 2, 13, 14 et 17 de la LPRPSP :

> **1.** La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.
>
> Elle s'applique à ces renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre.
>
> Elle s'applique aussi aux renseignements personnels détenus par un ordre professionnel dans la mesure prévue par le Code des professions (chapitre C-26).
>
> La présente loi ne s'applique pas à la collecte, la détention, l'utilisation ou la communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public.

---

[4] RLRQ c. P-40.1.

[5] La défenderesse demande l'exclusion des « non users » du groupe.

Les sections II et III de la présente loi ne s'appliquent pas à un renseignement personnel qui a un caractère public en vertu de la Loi.

2. Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.

13. Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie.

14. Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Un consentement qui n'est pas donné conformément au premier alinéa est sans effet.

17. La personne qui exploite une entreprise au Québec et qui communique à l'extérieur du Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer:

1° que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées sauf dans des cas similaires à ceux prévus par les articles 18 et 23;

2° dans le cas de listes nominatives, que les personnes concernées aient une occasion valable de refuser l'utilisation des renseignements personnels les concernant à des fins de prospection commerciale ou philanthropique et de faire retrancher, le cas échéant, ces renseignements de la liste.

Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1° et 2°, elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

[7] Voici les articles 35, 36, 37, 1457 et 1458 CcQ :

35. Toute personne a droit au respect de sa réputation et de sa vie privée.

Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise.

36. Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:

1° Pénétrer chez elle ou y prendre quoi que ce soit;

2° Intercepter ou utiliser volontairement une communication privée;

3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;

4° Surveiller sa vie privée par quelque moyen que ce soit;

5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;

6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

37. Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation.

1457. Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde.

1458. Toute personne a le devoir d'honorer les engagements qu'elle a contractés.

Elle est, lorsqu'elle manque à ce devoir, responsable du préjudice, corporel, moral ou matériel, qu'elle cause à son cocontractant et tenue de réparer ce préjudice; ni elle ni le cocontractant ne peuvent alors se soustraire à l'application des règles du régime contractuel de responsabilité pour opter en faveur de règles qui leur seraient plus profitables.

[8] Voici les articles 1, 5 et 49 de la Charte :

1. Tout être humain a droit à la vie, ainsi qu'à la sûreté, à l'intégrité et à la liberté de sa personne.

Il possède également la personnalité juridique.

5. Toute personne a droit au respect de sa vie privée.

49. Une atteinte illicite à un droit ou à une liberté reconnu par la présente Charte confère à la victime le droit d'obtenir la cessation de cette atteinte et la réparation du préjudice moral ou matériel qui en résulte.

En cas d'atteinte illicite et intentionnelle, le tribunal peut en outre condamner son auteur à des dommages-intérêts punitifs.

[9] Voici enfin les articles 219, 228 et 272 LPC :

219. Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur.

228. Aucun commerçant, fabricant ou publicitaire ne peut, dans une représentation qu'il fait à un consommateur, passer sous silence un fait important.

272. Si le commerçant ou le fabricant manque à une obligation que lui impose la présente loi, un règlement ou un engagement volontaire souscrit en vertu de l'article 314 ou dont l'application a été étendue par un décret pris en vertu de l'article 315.1, le consommateur, sous réserve des autres recours prévus par la présente loi, peut demander, selon le cas:

a) l'exécution de l'obligation;

b) l'autorisation de la faire exécuter aux frais du commerçant ou du fabricant;

c) la réduction de son obligation;

d) la résiliation du contrat;

e) la résolution du contrat; ou

f) la nullité du contrat,

sans préjudice de sa demande en dommages-intérêts dans tous les cas. Il peut également demander des dommages-intérêts punitifs.

[10] Le Tribunal va analyser plus loin si requis la portée de ces dispositions.

2.2 Les critères de l'article 575 Cpc

[11] L'autorisation d'exercer une action collective est accordée si chacun des quatre critères de l'article 575 Cpc est rempli. Cet article se lit ainsi :

> **575.** Le tribunal autorise l'exercice de l'action collective et attribue le statut de représentant au membre qu'il désigne s'il est d'avis que :
>
> 1. les demandes des membres soulèvent des questions de droit ou de fait identiques, similaires ou connexes;
>
> 2. les faits allégués paraissent justifier les conclusions recherchées;
>
> 3. la composition du groupe rend difficile ou peu pratique l'application des règles sur le mandat d'ester en justice pour le compte d'autrui ou sur la jonction d'instance;
>
> 4. le membre auquel il entend attribuer le statut de représentant est en mesure d'assurer une représentation adéquate des membres.

[12] Dans les arrêts *Infineon*[6], *Vivendi*[7], *Oratoire Saint-Joseph*[8] et *Asselin*[9], la Cour suprême du Canada a établi les principes suivants :

- L'autorisation d'un recours collectif au Québec nécessite l'atteinte d'un seuil peu élevé;

- Une fois les quatre conditions énoncées à 575 Cpc satisfaites, le juge d'autorisation doit autoriser le recours collectif; il ne bénéficie d'aucune discrétion résiduelle lui permettant de refuser l'autorisation au prétexte que, malgré l'atteinte de ces quatre conditions, le recours ne serait pas le véhicule « le plus adéquat »;

- La vocation de l'étape de l'autorisation du recours collectif est d'exercer une fonction de filtrage pour écarter les demandes frivoles, sans plus. L'exercice auquel le Tribunal est convié en est un de filtrage dont l'objectif est de se satisfaire de l'existence d'une cause défendable. Les conditions de l'article 575 Cpc doivent être appliquées de manière souple, libérale et généreuse afin de faciliter l'exercice de l'action collective comme moyen d'atteindre le double objectif de la dissuasion et de l'indemnisation des victimes. Tout doute doit jouer en faveur de l'autorisation;

- Quant à l'apparence de droit, le requérant n'a qu'un fardeau de démonstration et non de preuve. Il doit démontrer l'existence d'une « apparence sérieuse de droit », d'une « cause défendable »;

- Il n'y a aucune exigence au Québec que les questions communes soient prépondérantes par rapport aux questions individuelles. Au contraire, une seule question commune suffit si elle fait progresser le litige de façon non négligeable. Il n'est pas nécessaire que celle-ci soit déterminante pour le sort du litige;

---

6 *Infineon Technologies AG* c. *Option consommateurs*, 2013 CSC 59.
7 *Vivendi Canada inc.* c. *Dell'Aniello*, 2014 CSC 1.
8 *L'Oratoire Saint-Joseph du Mont-Royal* c. *J.J.*, 2019 CSC 35.
9 *Desjardins Cabinet de services financiers inc.* c. *Asselin*, 2020 CSC 30.

- Le Tribunal ne doit pas, à ce stade, se pencher sur le fond du litige et il doit prendre les faits pour avérés, sauf s'ils apparaissent invraisemblables ou manifestement inexacts. Le Tribunal doit prêter une attention particulière, non seulement aux faits allégués, mais aussi aux inférences ou présomptions de fait ou de droit qui sont susceptibles d'en découler et qui peuvent servir à établir l'existence d'une « cause défendable ».

[13] Il faut garder à l'esprit qu'avant le jugement d'autorisation, le recours n'existe pas sur une base collective[10]. C'est donc à la lumière du recours individuel de la personne demanderesse qu'il sera déterminé si les conditions de l'article 575 Cpc sont remplies[11].

[14] Le Tribunal reviendra plus loin sur certains autres principes applicables.

[15] Analysons maintenant les allégations du présent dossier au regard des quatre critères d'autorisation, en débutant par l'apparence de droit. C'est vraiment sur ce premier critère que porte le débat entre les parties.

[16] Rappelons ici que la défenderesse n'a pas eu la permission de déposer de la preuve[12].

2.3 Apparence de droit – 575 (2) Cpc

2.3.1 Précisions sur l'état du droit

[17] Le Tribunal débute par préciser la portée de la jurisprudence sur l'apparence de droit.

[18] Toutes les allégations de fait ne peuvent être tenues pour avérées. Les hypothèses, opinions, spéculations et inférences non supportées ne sont pas tenues pour avérées. De plus, les allégations factuelles générales qui visent le comportement d'une partie défenderesse ne peuvent être tenues pour avérées sans la présentation d'un élément de preuve. En effet, comme l'a établi la Cour suprême du Canada, lorsque des allégations de la demande sont générales et imprécises, elles sont insuffisantes pour satisfaire à la condition préliminaire d'établir une cause défendable; elles doivent être accompagnées d'une certaine preuve afin d'établir une cause défendable[13]. La Cour suprême du Canada l'a écrit ainsi dans l'arrêt *Oratoire Saint-Joseph*[14] :

> [59] En outre, à l'étape de l'autorisation, les faits allégués dans la demande sont tenus pour avérés, pourvu que les allégations de fait soient suffisamment précises : *Sibiga*, par. 52; *Infineon*, par. 67; *Harmegnies*, par. 44; *Regroupement des citoyens contre la pollution* c. *Alex Couture inc.*, 2007 QCCA 565, [2007]

---

10 *Bouchard* c. *Agropur Coopérative*, 2006 QCCA 1342, par. 109.
11 *Sofio* c. *Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820, par. 10.
12 *Homsy* c. *Google*, 2021 QCCS 4213.
13 Par. 134.
14 Précité, note 8, par. 59.

> R.J.Q. 859, par. 32; *Charles*, par. 43; *Toure,* par. 38; *Fortier*, par. 69. Lorsque des allégations de fait sont « vagues », « générales » ou « imprécises », elles se rapprochent nécessairement davantage de l'opinion ou de l'hypothèse, et elles peuvent donc difficilement être tenues pour avérées; elles doivent alors absolument « être accompagnées d'une certaine preuve afin d'établir une cause défendable » : *Infineon*, par. 134. De fait, l'arrêt *Infineon* suggère fortement au par. 134 (sinon explicitement, du moins implicitement) que de « simples allégations » — bien qu'« insuffisantes pour satisfaire à la condition préliminaire d'établir une cause défendable » (je souligne) — peuvent être complétées par une « certaine preuve » qui — « aussi limitée qu'elle puisse être » — doit accompagner la demande « afin d'établir une cause défendable ».

[19] Dans l'arrêt *Infineon*[15], la Cour suprême du Canada explique cette exigence, relativement à une allégation factuelle de complot entre les parties défenderesses :

> [134] À elles seules, ces simples allégations seraient insuffisantes pour satisfaire à la condition préliminaire d'établir une cause défendable. Bien que cette condition soit relativement peu exigeante, de simples affirmations sont insuffisantes sans quelque forme d'assise factuelle. Comme nous l'avons déjà souligné, les allégations de fait formulées par un requérant sont présumées vraies. Mais elles doivent tout de même être accompagnées d'une certaine preuve afin d'établir une cause défendable. Or, l'intimée a présenté une preuve, aussi limitée qu'elle puisse être, à l'appui de ses affirmations. Ainsi, les pièces attestent l'existence d'un complot visant la fixation des prix et de ses effets internationaux, qui ont été ressentis aux États-Unis et en Europe. À l'étape de l'autorisation, ces répercussions internationales apparentes du comportement anticoncurrentiel allégué des appelantes suffisent pour inférer que les membres du groupe auraient subi le préjudice allégué.

[20] Autrement dit, l'allégation suivante, sans aucune preuve, ne peut être tenue pour avérée : « les défendeurs ont fait un complot pour augmenter le prix de tel produit ».

[21] La Cour d'appel résume elle aussi ainsi cette exigence[16] :

> [40] Although the applicant only has a burden of demonstration at this stage, he must allege the facts that are relevant to his case and file the supporting evidence.

[22] Le Tribunal résume donc la portée de la jurisprudence :

- Une allégation générale visant le comportement d'une partie défenderesse ne peut être tenue pour avérée sans la présentation par le demandeur d'un élément de preuve. Tout fait ne doit cependant pas être supporté par un élément de preuve, car le Tribunal[17] peut faire des inférences ou tirer des présomptions de

---

15 Précité, note 6, par. 134.

16 *Ehouzou* c. *Manufacturers Life Insurance Company*, 2021 QCCA 1214, par. 40.

17 Voir par exemple *Morfonios (Succession de Sarlis)* c. *Vigi Santé ltée*, 2021 QCCS 2489, par. 67 et autorités citées.

fait ou de droit qui sont susceptibles de découler des éléments de preuve et qui peuvent servir à établir l'existence d'une cause défendable. L'exemple classique est la causalité;

- Une allégation relative à un élément factuel propre à un demandeur est tenue pour avérée, sauf si invraisemblable. Par exemple, l'allégation « La bouilloire que j'ai achetée ne fonctionne pas » doit être tenue pour avérée. L'allégation « J'ai été enlevé par des extra-terrestres » ne peut être tenue pour avérée car elle est invraisemblable. L'allégation « Ma bouilloire ne fonctionne pas car le fabricant a installé volontairement un élément chauffant défectueux » ne peut être tenue pour avérée sans aucun élément de preuve.

[23] Le Tribunal n'a pas ici à étudier l'impact de la preuve déposée par la défense car il n'y en a pas. Passons aux allégations du présent dossier.

2.3.2 Analyse des allégations du demandeur

[24] Le demandeur reproche à la défenderesse les deux pratiques factuelles suivantes :

- *Via* l'application Google Photos, avoir procédé à l'extraction, à la collecte, à la conservation et à l'utilisation des données biométriques faciales des résidents du Québec;

- Avoir omis et/ou négligé de décrire avec précision, voire d'informer le consommateur qu'elle procédait à l'extraction, la collecte, la conservation et l'utilisation de renseignements personnels sensibles sous forme de données biométriques faciales à partir des photos conservées sur sa plateforme Google Photos. Ceci aurait été fait sans fournir de préavis suffisant, sans obtenir un consentement éclairé et sans publier de politiques de conservation des données biométriques et ce, depuis octobre 2015.

[25] Le demandeur conclut que cela constitue les trois violations suivantes, soit les trois causes d'action :

- Avoir violé les articles 10, 13, 14 et 17 LPRPSP et les articles 35, 36, 37, 1457 et 1458 CcQ;

- Avoir sciemment porté atteinte aux droits à la vie privée et à l'inviolabilité des membres protégés par les articles 1 et 5 de la Charte;

- Avoir fait des représentations trompeuses aux utilisateurs de Google Photos au sujet de ses pratiques et politiques de confidentialité et ce, en violation des articles 219 et 228 LPC.

[26] Le demandeur réclame des dommages compensatoires en vertu de la LPRPSP, du CcQ et de la LPC, et également des dommages punitifs en vertu de l'article 272 LPC et de l'article 49 de la Charte.

[27] Le demandeur prétend que ses allégations démontrent une cause défendable, ce que nie la défenderesse.

[28] Étudions les allégations de la demande pour chaque pratique factuelle alléguée, pour ensuite étudier si requis les trois causes d'action.

2.3.2.1 Première pratique factuelle alléguée : extraction, collecte, conservation et utilisation des données biométriques faciales

[29] Le Tribunal étudie maintenant en détail tous les paragraphes pertinents de la Demande portant sur l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales par la défenderesse. Il s'agit d'analyser les paragraphes un par un, ou groupe par groupe, et ensuite si requis, de considérer leur effet cumulatif.

[30] Les deux premiers paragraphes[18] de la Demande sur cette pratique factuelle alléguée sont les suivants :

> 2. Since October 2015, Respondent, Google, LLC (the "Respondent"), has extracted, collected, stored, and used the facial biometric identifiers of tens of thousands of unwitting individuals throughout Quebec whose faces appear in photos uploaded to Google Photos, a cloud-based photo sharing and storage service included on all Android phones;
>
> 4. The Respondent engaged in its extraction, collection, and retention of Quebec residents' facial biometric data without providing any or adequate notice, obtaining informed consent, or publishing biometric data retention policies;

[31] De l'avis du Tribunal, les paragraphes 2 et 4 contiennent des allégations de fait générales sur le comportement et les agissements de la défenderesse dont le demandeur ne peut avoir une connaissance personnelle. Or, aucune preuve n'est apportée à leur soutien, si minimale soit-elle. Dans ces circonstances, en soi et pris isolément, ces deux paragraphes de la demande ne peuvent être tenus pour avérés. Il s'agit de paragraphes descriptifs de la théorie de la cause du demandeur.

[32] Les paragraphes 5 à 9 de la Demande sont une présentation proposée du groupe et un résumé des causes d'action du demandeur, des dommages réclamés, et ne contiennent pas des faits que le Tribunal peut tenir pour avérés.

---

[18] Le paragraphe 1 de la Demande est une présentation de la table des matières.

[33] Les paragraphes 10 et 11 de la Demande et la Pièce P-1 présentent les parties et ne contiennent aucuns faits relatifs aux causes d'action.

[34] Les paragraphes 3 et 12 à 21 de la Demande et les Pièces P-2 à P-4 décrivent diverses problématiques pouvant exister quant à l'extraction, à la collecte, à la conservation et à l'utilisation des données biométriques faciales. Des références sont faites aux trois documents suivants :

- Un guide de la Commission d'accès à l'information du Québec intitulé *Biométrie : principes à respecter et obligations légales des organisations* (Pièce P-2);

- L'*Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique* (Pièce P-3); et

- Projet de loi fédéral C-11 intitulé *Loi de 2020 sur la mise en œuvre de la Charte du numérique* (Pièce P-4).

[35] Or, les paragraphes 3 et 12 à 21 de la Demande et les Pièces P-2 à P-4 ne contiennent aucune référence à la défenderesse, ni de près, ni de loin, ni spécifiquement[19]. Donc en soi, sans rien d'autre, selon le Tribunal, ils ne peuvent constituer une preuve permettant de venir supporter une allégation de fait visant la défenderesse. En conséquence, outre les commentaires du Tribunal qui suivent quant à la Pièce P-3, les paragraphes 3 et 12 à 21 de la Demande et les Pièces P-2 à P-4 ne peuvent non plus supporter une quelconque présomption de fait ou inférence visant la défenderesse. De l'avis du Tribunal, il n'est donc aucunement requis ni utile de faire la description et l'étude des paragraphes 3 et 12 à 21 de la Demande et des Pièces P-2 à P-4.

[36] Cependant, le demandeur prétend que la défenderesse est directement impliquée par les notes 17 et 26 des paragraphes 38 et 65 de la Pièce P-3, dans laquelle les commissaires ont conclu que la Corporation Cadillac Fairview Limitée utilisait le logiciel FaceNet qui est un « reconnaisseur de visage » et permet de faire de la reconnaissance des visages. Les notes 17 et 26 citent un article de 2015[20] intitulé « FaceNet: A Unified Embedding for Face Recognition and Clustering » et rédigé par Florian Schroff, Dmitry Kalenichenko et James Philbin de Google Inc.

[37] Selon le demandeur :

- L'article Pièce P-8 a été rédigé par des employés de la défenderesse;

---

19 Le mot « Google » n'apparaît nulle part.

20 Personne n'a indiqué au Tribunal dans quelle parution cet article a été publié. Le texte de la Pièce P-8 ne permet pas de le dire. On peut lire dans la marge la référence suivante, qui ne permet de rien conclure : « arXiv:1503.03832v3 [cs.CV] 17 Jun 2015 ».

- L'article Pièce P-8 présente le logiciel de reconnaissance faciale FaceNet;

- L'article Pièce P-8 est rédigé avec l'emploi du mot « our » (notre) un peu partout;

- Le demandeur conclut que la défenderesse utilise le logiciel FaceNet;

- Par conséquent, tout ce que les commissaires ont conclu dans l'enquête Pièce P-3 quant à la Corporation Cadillac Fairview Limitée s'applique à la défenderesse.

[38] Avec égards, le Tribunal ne peut retenir cet argument. Voici pourquoi :

- Il est vrai que les auteurs de l'article Pièce P-8 sont identifiés comme appartenant à Google Inc., soit l'ancêtre de la défenderesse[21]. Cependant, nulle part est-il écrit dans la Pièce P-8 que la défenderesse utilise le logiciel FaceNet pour quelque usage que ce soit. Outre sous les noms des trois auteurs, le mot « Google » ou les mots « Google Photos » n'apparaissent pas. Le mot « GoogLeNet » apparaît à la page 4 mais le Tribunal n'a aucune idée de quoi il s'agit ni aucune compréhension du paragraphe technique dans lequel il se retrouve. Personne ne l'a expliqué à l'audition;

- Toutes les 48 références au mot « our » visent « our experiment », « our research » ou « our methods ». Il s'agit d'une qualification par les auteurs de leur algorithme, leur recherche, leur méthode. Il ne s'agit aucunement d'une mention selon laquelle la défenderesse utiliserait ce logiciel dans Google Photos ni même ailleurs dans ses produits;

- La section 7.2 « Summary » à la page 9 se conclut en indiquant qu'il serait souhaitable de tester le logiciel sur des petits réseaux. Autrement dit, rien n'est encore fonctionnel et l'article est une hypothèse de travail.

[39] Le Tribunal conclut donc que la Pièce P-8 ne constitue aucunement une « certaine preuve » permettant de soutenir l'allégation selon laquelle la défenderesse utilise le programme FaceNet dans Google Photos pour faire l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales. Par conséquence, la Pièce P-3 non plus ne peut être une « certaine preuve » pour soutenir les allégations du demandeur.

[40] En résumé, de l'avis du Tribunal, les paragraphes 3 et 12 à 21 de la Demande et les Pièces P-2 à P-4 ne supportent aucunement les allégations de fait du demandeur visant la défenderesse. Passons aux autres paragraphes de la Demande.

---

[21] On sait des Pièces P-9 et P-10 que Google Inc. est devenue Google LLC quelque part entre 2014 et 2017.

[41] Les paragraphes 22 à 36 de la Demande se lisent ainsi :

22. Google Photos is a cloud-based photo-sharing and storage service;

23. The Respondent first released Google Photos in the United States in May 2015. It later made the service available in Canada on or about October 28, 2015. Produced herewith as Exhibit P-5 is an article announcing the availability of Google Photos in Canada;

24. As of July 2019, Google Photos had over one billion users worldwide, as described in the article produced herewith as Exhibit P-6;

25. As of November 2020, more than 4 trillion photos were stored in Google Photos, and, every week 28 billion new photos and videos are uploaded, as described in the article produced herewith as Exhibit P-7;

26. The Google Photos application comes pre-installed on all Android phones, which are set by default to automatically upload photos taken by the user to the cloud-based service;

27. Android is the Respondent's smartphone operating system software;

28. Google Photos is also available for iOS, Apple's mobile operating system, and was accessible via web browsers;

29. Google Photos ran a proprietary neural network-based algorithm called FaceNet developed by the Respondent's researchers that had the highest accuracy in facial recognition at 99.63%. Produced herewith as Exhibit P-8 is an article describing the FaceNet technology;

30. Unbeknownst to Class Members, whenever a photo was uploaded to Google Photos, it was scanned for images of faces, and facial biometric identifiers were extracted from any detected face image;

31. Google Photos performed this extraction and collection of facial biometric identifiers without consideration for whether a particular face belonged to a Google Photos user or a non-user whose face happened to appear in the photo;

32. The facial biometric identifiers of the Applicant and other Class Members that were extracted and collected by the Respondent through Google Photos was stored and has remained accessible to the Respondent, its personnel, and any party that the Respondent permits to access such data including, but not limited to, third-party developers through application program interfaces, or "APIs";

33. The Respondent collected, stored, and used the facial biometric data of the plaintiff and other Class Members for its own competitive advantage in the marketplaces for photo-sharing and other services integrated with Google Photos, which services the Respondent has monetized, or may monetize, through data mining and targeted advertising;

> 34. Each Class Member had a right to control his or her own facial biometric identifiers. The Respondent did not obtain Class Members' consent to its extraction, collection, storage and use of facial biometric identifiers through Google Photos;
>
> 35. The Respondent never disclosed the specific purpose(s) and length of term for which Class Members' facial biometric identifiers would be extracted, collected, stored, and used;
>
> 36. The Respondent did not have any written, publicly available policies identifying its retention schedules, or guidelines for permanently destroying Class Members' biometric identifiers;

[42] Le Tribunal est d'avis que ces allégations ne démontrent aucune cause défendable. Il s'agit encore ici de généralités non supportées par un élément de preuve, donc non tenues pour avérées. Voici pourquoi.

1) Les paragraphes 22 et 23 décrivent les services offerts au Canada par la défenderesse et ne contiennent aucun reproche. Donc, ceci ne supporte pas les reproches du demandeur.

2) La Pièce P-5 est un article du 28 octobre 2015 de l'auteur Daniel Bader sur le site internet mobilesyrup.com. On y lit ceci :

> With version 1.8 on Android, Google Photos will now recognize faces and group them together under the Search button, a feature that was made available to American users after the service was unveiled at Google I/O this past May. With this version, facial tagging has been expanded to Latin America, Canada, the Caribbean, Australia, and New Zealand. The feature should also roll out to iOS users soon.
>
> The way it works sounds a bit creepy, but Google promises that it is not performing anything nefarious: it is merely matching traits of people uploaded to its servers in order to more easily identify them for tagging and sharing purposes. OK, that sounds more than a little creepy, these are things Google does better than anyone, requiring you to relinquish a bit of your privacy in the process.

3) Cet auteur indique donc que la version 1.8 de Google Photos va pouvoir reconnaître les données biométriques faciales des utilisateurs de Google Photos au Canada et les regrouper. Il s'agit donc d'un élément de preuve qui pourrait être considéré comme allant dans le sens de la théorie de la demande. Le Tribunal y revient plus loin.

4) Les paragraphes 24 et 25 de la Demande et les Pièces P-6 et P-7 sont descriptifs quant au nombre d'utilisateurs du service et au nombre de photos et ne contiennent aucune allégation reliée aux reproches du demandeur.

5) Les paragraphes 26, 27 et 28 sont également descriptifs quant à l'application Google Photo de la défenderesse et ne contiennent aucune allégation reliée aux reproches du demandeur.

6) Quant au paragraphe 29, il ne contient aucune allégation de fait visant la défenderesse. Quant à la Pièce P-8, le Tribunal l'a étudiée précédemment et a conclu qu'elle ne supporte pas les allégations du demandeur. Dans ces circonstances, ce paragraphe et cette Pièce ne peuvent être tenus pour avérés quant à la défenderesse.

7) Les paragraphes 30 à 36 ne contiennent aucun élément de preuve qui permet de justifier ce qui y est allégué. Toutes les allégations de ces paragraphes quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales par la défenderesse sont de la pure spéculation basée sur aucun élément de preuve. Elles ne peuvent être tenues pour avérées.

[43] Dans son plan d'argumentation, le demandeur fait référence au document suivant : *Rapport de conclusions, Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta, Section surveillance, 1023158-S*. Or, le Tribunal ne peut tenir compte de ce document puisqu'il ne fait pas partie de la preuve jointe à la Demande. En effet, les faits ne peuvent provenir d'un plan d'argumentation de la demande[22], mais doivent être allégués de façon formelle à une demande pour autorisation d'exercer une action collective[23].

[44] Donc, quant à la première pratique factuelle alléguée par le demandeur, de toutes les allégations du demandeur dans la Demande, aucune n'est supportée par un quelconque élément de preuve, sauf quant à la Pièce P-5. Le seul élément de preuve qui existe est celui contenu dans la Pièce P-5, dans lequel un auteur a écrit les extraits suivants, une fois qu'on enlève les commentaires éditoriaux :

> [...] Google Photos will now recognize faces and group them together under the Search button, [...]. With this version, facial tagging has been expanded to [...] Canada [...].
>
> [...] Google promises that it is not performing anything nefarious: it is merely matching traits of people uploaded to its servers in order to more easily identify them for tagging and sharing purposes. [...].

---

22 *Li* c. *Equifax inc.*, 2019 QCCS 4340, par. 41; *Labbé* c. *Centre de services scolaires des Samares*, 2022 QCCS 517, par. 32.

23 Dès son dépôt initial ou par modification subséquente avec la permission du Tribunal.

[45] De l'avis du Tribunal, cela est nettement insuffisant pour établir l'existence d'une pratique généralisée par la défenderesse d'extraction, de collecte, de conservation et d'utilisation des données biométriques faciales par la défenderesse. De l'avis du Tribunal, deux phrases tirées d'un article d'un auteur dont on ne connaît aucunement la compétence, le statut ou les qualifications, et sur un site internet dont on ne connaît rien quant au statut ni à la diffusion, ne permettent pas de constituer une preuve suffisante à établir une allégation factuelle qu'on peut tenir pour avérée. Cet article constitue tout simplement l'opinion d'un auteur dont on ne sait rien; on ne peut conclure qu'il s'agit d'une publication scientifique rigoureuse ou d'une enquête journalistique suffisante. On ne sait pas s'il s'agit d'un vrai journaliste ou d'un bloggeur ou d'une personne dans son sous-sol qui écrit ce qu'il lui passe par la tête. Sans nécessiter une preuve ou description étendue, le demandeur devait quand même expliquer ces éléments.

[46] Par ailleurs, même en supposant qu'il soit valide comme « certaine preuve » – ce qu'il n'est pas - le texte de la Pièce P-5 est plutôt laconique et avare de détails spécifiques quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales. De l'avis du Tribunal, son absence de détail confirme qu'il s'agit de l'opinion personnelle de l'auteur.

[47] Le Tribunal conclut qu'accepter la Pièce P-5 comme étant une « certaine preuve » n'est pas possible dans ces circonstances. Conclure autrement signifierait qu'il serait possible de déclencher une action collective sur de simples soupçons ou d'articles d'opinion d'auteurs inconnus et invérifiables.

[48] Par comparaison, dans l'arrêt *Infineon*, la Cour suprême du Canada a décidé qu'il y avait une preuve suffisante de l'existence d'un complot. Il n'y avait pas juste des articles d'auteurs inconnus qui disaient qu'il y avait un complot.

[49] Le Tribunal ajoute qu'il ne porte aucune attention aux commentaires de personnes non identifiées[24] qui apparaissent à la fin de la Pièce P-5.

[50] Passons aux autres paragraphes pertinents de la Demande.

[51] Les paragraphes 45 à 59 de la Demande font état des faits propres au demandeur et ne contiennent aucun élément de preuve additionnel. Ces allégations se basent sur les précédentes, lesquelles sont insuffisantes puisque sans preuve suffisante, de l'avis du Tribunal.

[52] Le Tribunal conclut que, dans ces circonstances, que ce soit de façon individuelle ou même par leur effet cumulatif, les allégations du demandeur sur sa première allégation de pratique factuelle de la défenderesse ne peuvent être tenues pour avérées. Le demandeur n'a donc pas démontré une cause défendable quant à l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales par la défenderesse.

---

[24] Comme par exemple « FlamesFan89 » ou « selon moi ».

[53] Dans ces circonstances, tout le reste de la Demande n'a plus de conséquence et ne peut générer une quelconque responsabilité de la défenderesse, car tous les autres reproches du demandeur supposent que la défenderesse fasse l'extraction, la collecte, la conservation et l'utilisation des données biométriques faciales. Or, le demandeur ne l'a pas démontré.

[54] Autrement dit, puisque le demandeur n'a pas démontré l'existence de la pratique alléguée d'extraction, de collecte, de conservation et d'utilisation des données biométriques faciales, il est donc inutile de savoir si la défenderesse a fourni ou non de préavis suffisant ou a obtenu le consentement du demandeur et des membres du groupe ou leur a fait des fausses représentations. Également, pour les mêmes raisons, il ne peut y avoir de dommages punitifs[25].

2.3.2.2 Deuxième pratique factuelle alléguée : ne pas avoir fourni de préavis suffisant, ni d'avoir obtenu un consentement éclairé ni d'avoir publié des politiques de conservation des données biométriques

[55] Il n'est donc pas requis que le Tribunal procède à cette analyse.

[56] Dans ces circonstances, le Tribunal conclut que le demandeur n'a pas démontré une violation des articles 10, 13, 14 et 17 LPRPSP, ni une violation des articles 35, 36, 37, 1457 et 1458 CcQ, ni une violation des droits à la vie privée et à l'inviolabilité des membres protégés par les articles 1 et 5 de la Charte, ni d'avoir fait des représentations trompeuses aux utilisateurs de Google Photos au sujet de ses pratiques et politiques de confidentialité en violation des articles 219 et 228 LPC. Sans la démonstration des faits à la base de la théorie du demandeur, tout doit tomber, incluant les allégations reliées aux dommages punitifs.

[57] Les paragraphes 68 à 79 de la Demande sont des conclusions juridiques qui ne sont pas supportées par une démonstration des faits à leur base.

[58] Le Tribunal n'a donc pas à étudier non plus les allégations relatives aux dommages compensatoires et aux dommages punitifs.

2.3.3 Conclusion

[59] Le demandeur n'a pas démontré de cause défendable. La Demande doit donc être rejetée pour ce simple motif.

---

[25] Même de façon autonome : le demandeur n'a pas établi que la défenderesse a commis la pratique dont il se plaint.

2.4 Questions identiques, similaires ou connexes – 575(1) Cpc

[60] La présence de questions identiques, similaires ou connexes n'est pas contestée ici par la défenderesse. S'il y avait eu apparence de droit, le Tribunal aurait conclu que les questions proposées par le demandeur au paragraphe 82 de la Demande sont identiques, similaires ou connexes.

2.5 Composition du groupe – 575(3) Cpc

[61] Les éléments généralement considérés dans l'analyse de cette condition de l'article 575 Cpc sont les suivants[26] :

- Le nombre probable de membres;
- La situation géographique des membres; et
- Les contraintes pratiques et juridiques inhérentes à l'utilisation du mandat et de la jonction des parties en comparaison avec l'action collective.

[62] La défenderesse ne conteste pas que l'article 575(3) Cpc est satisfait ici. S'il y avait eu apparence de droit, le Tribunal aurait conclu que les paragraphes 86 à 98 de la Demande remplissent ce critère.

2.6 Représentant – 575(4) Cpc

[63] La Cour d'appel a récemment réitéré les critères à étudier pour décider de la capacité du représentant aux termes du paragraphe 4 de l'article 575 Cpc[27]:

> [30] ... cette condition requiert la démonstration que (le demandeur) a l'intérêt d'agir, qu'il en a la compétence et, enfin, qu'il n'existe aucun conflit entre celui-ci et les membres du groupe.

[64] Outre l'absence d'intérêt lié à l'absence d'apparence de droit, la défenderesse ne conteste pas que l'article 575(4) Cpc est satisfait ici. S'il y avait eu apparence de droit, le Tribunal aurait conclu que les paragraphes 99 à 109 de la Demande remplissent ce critère.

2.7 Autres éléments

[65] Compte tenu de ce qui précède, le Tribunal n'a pas à étudier ici la redéfinition du groupe, l'inclusion ou l'exclusion dans le groupe des « non users », le point de départ du

---

[26] Yves LAUZON, *Le recours collectif*, Cowansville, Éditions Yvon Blais, 2001, p. 38; *Brière* c. *Rogers Communications*, 2012 QCCS 2733, par. 72.

[27] *Tenzer* c. *Huawei Technologies Canada Co. Ltd.*, 2020 QCCA 633.

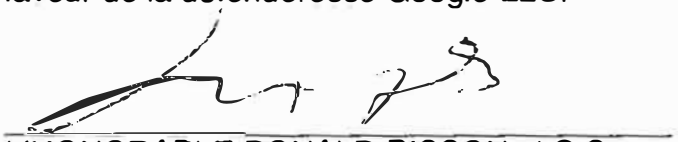
groupe, la fermeture ou non du groupe, la redéfinition potentielle des questions identiques, similaires ou connexes proposées, ni les questions du district judiciaire et des avis.

[66] Quant aux frais de justice, le Tribunal les octroie à la défenderesse qui a gain de cause.

POUR CES MOTIFS, LE TRIBUNAL :

[67] **REJETTE** l'*Originating Application for Authorization to Institute a Class Action and to Obtain the Status of Representative* du demandeur Michael Homsy;

[68] **LE TOUT**, avec frais de justice en faveur de la défenderesse Google LLC.



L'HONORABLE DONALD BISSON, J.C.S.

Me Jean-Philippe Caron, Me Alessandra Esposito Chartrand, Me Gabriel Bois et
M. Benjamin Tavernier-Labrie, stagiaire
CALEX LEGAL INC.
Avocats du demandeur Michael Homsy

Me John Archibald
INVESTIGATION COUNSEL PC
Avocat du demandeur Michael Homsy

Me Noah Michael Boudreau et Me Mirna Kaddis
FASKEN MARTINEAU DUMOULIN SENCRL, S.R.L.
Avocats de la défenderesse Google LLC

Date d'audition : 21 février 2022

ANNEXE 2

C A N A D A

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

S U P E R I O R C O U R T
(Class Action)

NO.: **500-06-001123-211**

MICHAEL HOMSY, residing at [redacted]

Applicant

-vs-

GOOGLE LLC., a legal person, duly constituted according to law, with its head office located at 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA

Respondent

ORIGINATING APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION AND TO OBTAIN THE STATUS OF REPRESENTATIVE
(Articles 574 and following C.C.P.)

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT, SITTING IN AND FOR THE DISTRICT OF MONTREAL, APPLICANT RESPECTFULLY SUBMITS THE FOLLOWING:

A. SUMMARY

1. This Application shall be presented in the following matter:

v. The Claims of Each Class Member

E. THE RESPONDENT'S LIABILITY

i. Breach of obligations stemming from of the *PPIPS* and the *CCQ*
ii. Breach of obligations under the *Charter*
iii. Breach of obligations under the *Consumer Protection Act*

F. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION (art. 575 *CCP*)

i. The claims of the members of the Class raise identical, similar or related issues of law or fact (art. 575 (1) *CCP*)
ii. The facts alleged appear to justify the conclusions sought (art. 575 (2) *CCP*)
iii. The composition of the Class makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (art. 575 (3) *CCP*)
iv. The Applicant is in a position to properly represent the Class Members (art. 575 (4) *CCP*)

G. JUDICIAL DISTRICT

B. GENERAL PRESENTATION

2. Since October 2015, Respondent, Google, LLC (the "**Respondent**"), has extracted, collected, stored, and used the facial biometric identifiers of tens of thousands of unwitting individuals throughout Quebec whose faces appear in photos uploaded to Google Photos, a cloud-based photo sharing and storage service included on all Android phones;

3. Facial biometric identifiers are biologically unique and intrinsically private to each Class Member. Like fingerprints and DNA, they enable the identification of an individual with precision in a wide range of circumstances;

4. The Respondent engaged in its extraction, collection, and retention of Quebec residents' facial biometric data without providing any or adequate notice, obtaining informed consent, or publishing biometric data retention policies;

5. Applicant Michael Homsy (hereinafter referred to the "**Applicant**'") wishes to institute a class action on behalf of the following sub-classes of persons (collectively, the "**Class**" or "**Class Members**"):

> **User Class:** All individuals residing in the Province of Quebec, except for the Excluded Persons*, who used Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos since October 28th, 2015 (the "**Class Period**");

Non-User Class: All individuals residing in the Province of Quebec, except for the Excluded Persons, who did not use Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos during the Class Period;

*"**Excluded Persons**" means Google and its parent corporations, subsidiaries, affiliates, predecessors, successors and assigns; and their current or former officers, directors, and legal representatives;

6. The Applicant alleges that the Respondent violated Class Members' rights to inviolability and privacy under the *Charter of human rights and freedoms*, CQLR c C-12 ("***Charter***");

7. He alleges that the Respondent acted unlawfully and with knowledge that its conduct would violate individuals' privacy and inviolability rights. In particular, the Respondent failed to meet its obligations under the *Civil Code of Quebec*, CQLR c CCQ-1991 (the "***CCQ***") and the *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 (the "***PPIPS***"), which inform the scope and content of the Respondent's obligations under the *Charter*;

8. The Applicant further alleges that, in violation of the *Consumer Protection Act*, CQLR, c P-40.1 ("***Consumer Protection Act***"), the Respondent made representations to the users of Google Photos about its privacy practices and policies that were misleading because they omitted, or were otherwise ambiguous about, the material fact of the Respondent's collection and retention of sensitive personal information in the form of facial biometric data;

9. This class action seeks an award of moral damages for Class Members' inconvenience and anxiety and for the vindication of their rights, an award of material damages for sums spent by Class Members in order to store their photos on an alternative platform in order to protect their privacy and inviolability, and an award of punitive damages sufficient to condemn the Respondent's unlawful conduct, impose a just penalty, and deter future breaches of Class Members' rights;

C. THE PARTIES

10. The Applicant, Michael Homsy, is an individual who lives in Vaudreuil-Dorion, Quebec;

11. The Respondent is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043, USA, the whole as appears from the corporate search results disclosed as **Exhibit P-1**. The Respondent carries on business worldwide, including in Quebec and Canada. Google is a subsidiary of Alphabet Inc;

D. THE FACTS

i. Biometric identifiers implicate privacy and integrity concerns

12. "*Biometrics*" are unique physical characteristics used to identify an individual;

13. The *Commission d'accès à l'information du Quebec* has published guidance on biometrics, reproduced as **Exhibit P-2,** that clearly affirms that biometric information is personal;

14. An investigation report published on October 28, 2020 by the Privacy Commissioner of Canada and privacy commissioners in Alberta and British Columbia, reproduced as **Exhibit P-3**, stated that biometric data is "is distinctive, stable over time, difficult to change and largely unique to the individual";

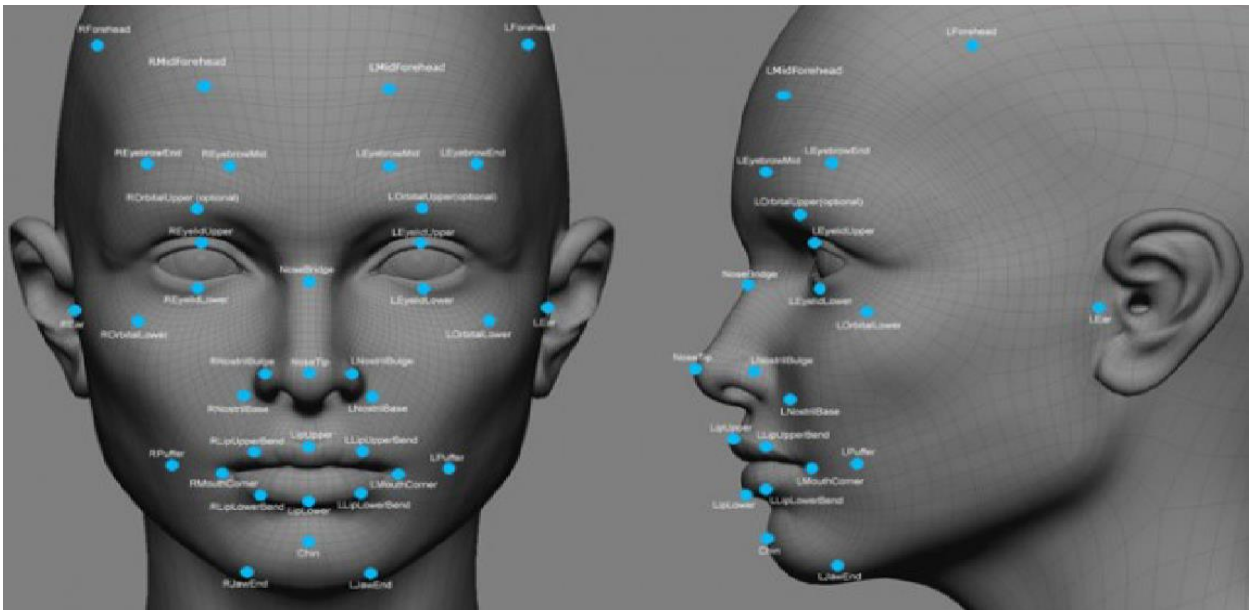
15. Within the category of biometrics, there are degrees of data sensitivity. According to Canadian privacy commissioners, facial biometric data is more sensitive because its possession can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance (**Exhibit P-3**);

16. As a result, the use of facial recognition technology in the commercial context has been recognized as presenting serious consumer inviolability and privacy concerns (**Exhibit P-3**);

17. Facial recognition technology works by capturing images that are converted and encoded through the computation of a series of measurements of the human face's geometry as determined by facial points and contours;

18. This embedding process generates biometric data in the form of a numerical representation of the human face. An individual can then be identified when the unique biometric representation of his or her face is compared against others in a database;

19. The following is an example of geometric data points of a human face:



20. Canadian privacy commissioners have underscored the importance of companies' obtaining an individual's express, opt-in consent before extracting and collecting the individual's facial biometric identifiers (**Exhibit P-3**);

21. The importance of the privacy concerns raised by the exploitation of data in the private sector, including biometric data, is further highlighted in the government of Canada' proposition of the Digital Charter Implementation Act, 2020 (Bill C-11, reproduced as exhibit **P-4**), published on November 17 2020, which seeks to implement the *Canadian Digital Charter and the Consumer Privacy Protection Act*, in order to increase Canadians' control over their data and information;

ii. The Respondent's Extraction, Collection, and Retention of Facial Biometric Identifiers

22. Google Photos is a cloud-based photo-sharing and storage service;

23. The Respondent first released Google Photos in the United States in May 2015. It later made the service available in Canada on or about October 28, 2015. Produced herewith as **Exhibit P-5** is an article announcing the availability of Google Photos in Canada;

24. As of July 2019, Google Photos had over one billion users worldwide, as described in the article produced herewith as **Exhibit P-6**;

25. As of November 2020, more than 4 trillion photos were stored in Google Photos, and, every week 28 billion new photos and videos are uploaded, as described in the article produced herewith as Exhibit **P-7**;

26. The Google Photos application comes pre-installed on all Android phones, which are set by default to automatically upload photos taken by the user to the cloud-based service;

27. Android is the Respondent's smartphone operating system software;

28. Google Photos is also available for iOS, Apple's mobile operating system, and was accessible via web browsers;

29. Google Photos ran a proprietary neural network-based algorithm called FaceNet developed by the Respondent's researchers that had the highest accuracy in facial recognition at 99.63%. Produced herewith as **Exhibit P-8** is an article describing the FaceNet technology;

30. Unbeknownst to Class Members, whenever a photo was uploaded to Google Photos, it was scanned for images of faces, and facial biometric identifiers were extracted from any detected face image;

31. Google Photos performed this extraction and collection of facial biometric identifiers without consideration for whether a particular face belonged to a Google Photos user or a non-user whose face happened to appear in the photo;

32. The facial biometric identifiers of the Applicant and other Class Members that were extracted and collected by the Respondent through Google Photos was stored and has remained accessible to the Respondent, its personnel, and any party that the Respondent permits to access such data including, but not limited to, third-party developers through application program interfaces, or "APIs";

33. The Respondent collected, stored, and used the facial biometric data of the plaintiff and other Class Members for its own competitive advantage in the marketplaces for photo-sharing and other services integrated with Google Photos, which services the Respondent has monetized, or may monetize, through data mining and targeted advertising;

34. Each Class Member had a right to control his or her own facial biometric identifiers. The Respondent did not obtain Class Members' consent to its extraction, collection, storage and use of facial biometric identifiers through Google Photos;

35. The Respondent never disclosed the specific purpose(s) and length of term for which Class Members' facial biometric identifiers would be extracted, collected, stored, and used;

36. The Respondent did not have any written, publicly available policies identifying its retention schedules, or guidelines for permanently destroying Class Members' biometric identifiers;

iii. The Respondent's Privacy Misrepresentations

37. During the Class Period, the Respondent made representations in its terms of service and in its privacy policies about the nature of the personal information it collected, how it collected that information, and how its services used "*pattern recognition*";

38. Produced herewith are the versions of the Respondent's Terms of Service applicable to Google Photos during the Class Period, with the effective dates April 30, 2014 (**Exhibit P-9**); October 25, 2017 (**Exhibit P-10**); and March 31, 2020 (**Exhibit P-11**);

39. Produced herewith are certain versions of the Respondent's Privacy Policy during the Class Period, with the effective dates of August 19, 2015 (**Exhibit P-12**); March 25, 2016 (**Exhibit P-13**); May 25, 2018 (**Exhibit P-14**); and September 30, 2020 (**Exhibit P-15**);

40. Produced herewith as **Exhibit P-16** is a page from the Respondent's websites entitled "Key Terms" which provides definitions of "personal information" and "sensitive personal information";

41. Produced herewith as **Exhibit P-17** is a page from the Respondent's website entitled "Our Privacy and Security Principles";

42. Produced herewith as **Exhibit P-18** is a page from the Respondent's website entitled "How Google uses pattern recognition to make sense of images";

43. The Respondent's representations were misleading because they omitted, or otherwise used ambiguity about, the material fact that the Respondent was extracting, collecting,

storing, and using Class Members' personal information in the form of facial biometric identifiers (the "**Privacy Misrepresentations**");

44. The Privacy Misrepresentations included the following:

- "We build privacy that works for you … We keep you informed about what data we collect, how it's used, and why.";

- "Be clear about what data we collect and why … To help people make informed decisions about how they use Google products, we make it easy to understand what data we collect, how it's used, and why. Being transparent means making this information readily available, understandable, and actionable.";

- "[Personal information] is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.";

- "Information Google collects … We want you to understand the types of information we collect as you use our services. We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.
  …

  Things you create or provide to us … When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to receive updates about our services.

  We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.";

- "We collect information in two ways:

  Information you give us.

  For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google

Profile, which may include your name and photo.

Information we get from your use of our services.

We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or you view and interact with our ads and content. This information includes:

Device information

[…]

Log information

[…]

Internet protocol address

[…]

Location information

[…]

Unique application numbers

[…]

Local storage

[…]

Cookies and anonymous identifiers

[…]";

- "How Google uses pattern recognition to make sense of images…Computers don't 'see' photos and videos in the same way that people do. When you look at a photo, you might see your best friend standing in front of her house. From a computer's perspective, that same image is simply a bunch of data that it may interpret as shapes and information about color values. While a computer won't react like you do when you see that photo, a computer can be trained to recognize certain patterns of color and shapes.

  A computer might also be trained to recognize the common patterns of shapes and colors that make up a digital image of a face. This process is known as face

> detection, and it's the technology that helps Google to protect your privacy on services like Street View, where computers try to detect and then blur the faces of any people that may have been standing on the street as the Street View car drove by.
>
> If you get a little more advanced, the same pattern recognition technology that powers face detection can help a computer to understand characteristics of the face it has detected. For example, there might be certain patterns that suggest a face is smiling or has its eyes closed. Information like this can be used to help with features like Google Photos' suggestions of movies and other effects created from your photos and videos.
>
> Similar technology also powers the face grouping feature available in Google Photos in certain countries, which helps computers detect similar faces and group them together, making it easier for users to search and manage their photos.";

iv. The Applicant's Personal Claims

45. The facts upon which the Applicant's personal claims against the Respondent are based are as follows;

46. The Applicant is a resident of Vaudreuil-Dorion, Quebec, in the greater Montreal area;

47. The Applicant used an Android phone during the Class Period;

48. On or about the month of March 2020 the Applicant purchased an Android phone and began using Google Photos;

49. When the Applicant started using Google Photos, he accepted the Respondent's Terms of Use and Privacy Policy;

50. The Applicant took photos of himself and others using his Android phone and uploaded them to Google Photos;

51. Since the Applicant started using Google Photos, he has uploaded an estimated 5,500 photos to the platform;

52. At no time did the Applicant know that the Respondent was extracting, collecting, storing, and using facial biometric identifiers from his photos;

53. The Applicant was made aware of the Respondent's illegal storage and use of his facial biometric data during the month of January 2021;

54. Therefore, the Respondent engaged in these practices without the Applicant's knowledge and consent;

55. Had the Applicant been made aware that the Respondent was illegally storing and using his facial biometric data, the Applicant would not have used the Google Photos application on his phone to store his personal photos;

56. Indeed, soon after realizing that the Respondent was illegally storing and using his facial biometric data, the Applicant transferred his photos to an alternative cloud-based photo sharing and storage service, Dropbox;

57. Produced herewith as **Exhibit P-19** is a receipt confirming the applicant's subscription to Dropbox cloud storage as of January 14, which forced the defendant to pay an annual amount of 171,44$;

58. As a result of the Respondent's blatant violation of the Applicant's right to privacy and inviolability, the Applicant suffered damages, including inconvenience, anxiety and pecuniary damages;

59. At the thought of his personal biometric data being in the hands of third parties with no control on its use, the Applicant has been overcome with feelings of powerlessness, betrayal, fear, stress, and anxiety;

v. The Claims of Each Class Member

60. The facts giving rise to personal claims by each of the members of the Class against the Respondent are as follows;

61. Every member of the Class had their facial biometric data extracted from photos uploaded on Google Photos which data was collected, stored, and used by the Respondent;

62. Every Class Member had a privacy interest in his or her facial biometric data;

63. Every Class Member's right to integrity was violated by the collection of his or her facial biometric data;

64. Each Class Member did not consent to the collection, retention, and use of their facial biometric identifiers by the Respondent;

65. Each Class Member's inviolability and privacy rights were violated by the Respondent's unlawful, unfair, abusive and/or misleading acts and practices and intentional and malicious conduct;

66. The Class Members each suffered damages, including inconvenience and anxiety;

67. Some Class Members have bought a subscription to an alternative cloud-based photo sharing and storage service;

E. THE RESPONDENT'S LIABILITY

i. Breach of obligations stemming from of the *PPIPS* and the *CCQ*

68. The Applicant and Class Members' facial biometric data, which was extracted, collected, retained, used and made accessible to third parties by the Defendant, is "personal information" as provided for by the *PPIPS*;

69. The Respondent was therefore subject to the obligations in the *PPIPS* in respect of its collection, retention, and use of the personal information of both users and non-users of Google Photos and had the obligation to protect, and not to misuse, their personal information;

70. The Respondent breached its obligations by extracting, collecting, retaining, and using, the Applicant and Class Members' personal information, in the form of their facial biometric identifiers, without their consent and without ever disclosing its actions to them;

71. More particularly, the Respondent breached its obligations under articles 10 and 13, 14 and 17 of *PPIPS* and articles 35 to 37, and 1457 and/or 1458 of the *CCQ*;

72. As a result of the Respondent's breaches, the Applicant and other Class Members are entitled to damages;

ii. Breach of obligations under the *Charter*

73. The Respondent's conduct, as set out above, also breached the Applicant and Class Members' rights to inviolability and respect for their private lives as guaranteed by articles 1 and 5 of the *Charter*;

74. The Respondent extracted, collected, stored and used highly sensitive personal information, namely facial biometric data, without the consent of Class Members and intentionally omitted to disclose these practices to them;

75. The Respondent chose to put its own financial interests before the interests of the Applicant and the Class Members. It showed a disregard of the rights of both users and non-users of Google Photos who unwittingly had sensitive personal information collected from them;

76. This unlawful and intentional interference with its users' rights warrants an award of punitive damages under article 49 of the *Charter*;

iii. Breach of obligations under the *Consumer Protection Act*

77. Through its actions as set out above, Google breached the *Consumer Protection Act*;

78. The Respondent breached articles 219 and 228 of the *Consumer Protection Act* by making the Privacy Misrepresentations, which were misleading to the Applicant and other Class Members because they omitted, or otherwise used ambiguity as to, the material fact that

Google was extracting, collecting, storing, and using the facial biometric identifiers of both users and non-users of Google Photos;

79. The Respondent's conduct warrants an award of punitive damages under article 272 of the *Consumer Protection Act*;

F. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION (art. 575 *CCP)*

i. The claims of the members of the Class raise identical, similar or related issues of law or fact (art. 575 (1) *CCP*)

80. Individual issues, if any, pale by comparison to the numerous common issues that are significant to the outcome of the litigation;

81. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely, the Respondent's misconduct;

82. The claims of the members raise identical, similar or related issues of fact or law, namely:

A. Did the Respondent breach articles 3,10, 35, 36, and/or 37, and 1457 and/or 1458 of the *CCQ*?

B. Did the Respondent breach its statutory obligations under the *PPIPS*?

C. Did the Respondent breach articles 1 and/or 5 of the *Charter*?

D. Did the Respondent breach articles 219 and 228 of the *Consumer Protection Act*?

E. Are Class Members entitled to material and/or moral damages?

F. Are Class Members entitled to punitive damages?

G. What are the amounts of the aggregate moral, material and punitive damages to be awarded to the Class?

ii. The facts alleged appear to justify the conclusions sought (art. 575 (2) *CCP*)

83. In this regard, the Applicant refers to paragraphs 2 to 79 of this Application;

84. The action that the Applicant wishes to institute on behalf of the members of the Class is:

An action in damages against the Respondent in reparation of the harm caused by the Respondent's unlawful violation of the Class Member's right to privacy and inviolability, and its misrepresentations and omissions regarding the privacy features of its Google Photos application.

85. The conclusions that the Applicant wishes to introduce by way of an application to institute

proceedings are:

a. **GRANT** the applicant's action against the Respondent;

b. **DECLARE** that the Respondent:

i. Violated its statutory obligations under the *CCQ* and the *PPIPS*;

ii. Intentionally and unlawfully violated class members' rights to privacy and inviolability under the *Charter*;

iii. Violated its statutory obligations under the *Consumer Protection Act*;

c. **CONDEMN** the Respondent to pay the Class Members material, moral and punitive damages in amounts to be determined by the Court based on the evidence at trial;

d. **ORDER** collective recovery in accordance with articles 595-598 of the *CCP* for the moral and punitive damages, and individual recovery in accordance with articles 599-601 of the *CCP* for the material damages;

e. **CONDEMN** the Respondent to any other remedy deemed appropriate, just, and reasonable;

THE WHOLE with legal costs, including the costs of all publications of notices, experts and expert reports and the attendance fees of the experts to present these reports in Court;

iii. The composition of the Class makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (art. 575 (3) *CCP*)

86. The Applicant is not privy to the specific number of persons residing in Quebec whose facial biometric data were extracted and collected by the Respondent through Google Photos;

87. However, given that Google Photos is pre-installed on devices using the Android operating system, which is used by approximately half of Canadians, it is reasonable to assume that the Class number is in the tens of thousands;

88. Further, the Defendant's electronic databases could easily establish the number of Class Members;

89. Class Members are numerous and are scattered across the entire province;

90. In addition, given the costs and risks inherent in an action before the courts, many people will hesitate to institute an individual action against the Respondent;

91. Even if the Class Members themselves could afford such individual litigation, it would place

an unjustifiable burden on the courts and, at the very least, is not in the interests of judicial economy;

92. Furthermore, individual litigation of the factual and legal issues raised by the conduct of the Respondent would increase delay and expense to all parties and to the court system;

93. By their very nature, wrongdoing in the smartphone market affects many individuals and any discrepancies tend to be quite small – if it were not for the class action mechanism which facilitates access to justice, these types of claims would never be heard;

94. It is expected that the majority of Class Members have suffered small losses making it economically unfeasible to finance the litigation expenses inherent in any legal proceeding;

95. This class action overcomes the dilemma inherent in an individual action whereby the legal fees alone would deter recovery and thereby in empowering the consumer, it realizes both individual and social justice as well as rectifies the imbalance and restores the parties to parity;

96. Also, a multitude of actions instituted in either the same or different judicial districts, risks having contradictory judgments on questions of fact and law that are similar or related to all members of the Class;

97. These facts demonstrate that it would be impractical, if not impossible, to contact each and every member of the Class to obtain mandates and to join them together into one action;

98. In these circumstances, a class action is the only appropriate procedure and the only viable means for all of the members of the Class to effectively pursue their respective legal rights and have access to justice;

iv. The Applicant is in a position to properly represent the Class Members (art. 575 (4) *CCP*)

99. The Applicant is a member of the Class;

100. The Applicant is ready and available to manage and direct the present action in the interest of the members of the Class that he wishes to represent and is determined to lead the present action until a final resolution of the matter, the whole for the benefit of the Class, as well as and to dedicate the time necessary for the present action before the Courts, as the case may be, and to collaborate with his attorneys;

101. The Applicant has the capacity and interest to fairly, properly, and adequately protect and represent the interest of the members of the Class;

102. The Applicant has given the mandate to his attorneys to obtain all relevant information with respect to the present action and intends to keep informed of all developments;

103. The Applicant, with the assistance of his attorneys, is ready and available to dedicate the

time necessary for this action and to collaborate with other members of the Class and to keep them informed;

104. The Applicant has given instructions to his attorneys to put information about this class action on its website and to collect the coordinates of those Class Members that wish to be kept informed and participate in any resolution of the present matter, the whole as will be shown at the hearing;

105. The Applicant has also given instructions to his attorneys to create a *Facebook* page allowing the Class Members to be kept informed of the evolution of the present matter;

106. The Applicant is in good faith and has instituted this action for the sole goal of having his rights, as well as the rights of other Class Members, recognized and protected so that they may be compensated for the damages that they have suffered as a consequence of the Respondent's conduct;

107. The Applicant understands the nature of the action;

108. The Applicant's interests do not conflict with the interests of other Class Members and further Applicant has no interest that is antagonistic to those of other members of the Class;

109. The Applicant is prepared to be examined out-of-court on his allegations (as may be authorized by the Court) and to be present for Court hearings, as may be required and necessary;

G. JUDICIAL DISTRICT

110. The Applicant suggests that this class action be exercised before the Superior Court in the district of Montreal;

111. A great number of the members of the Class reside in the judicial district of Montreal;

112. Some of the Applicant's attorneys practice their profession in the judicial district of Montreal;

113. The present application is well founded in fact and in law;

WHEREFORE THE APPLICANT PRAYS THAT BY JUDGMENT TO BE RENDERED HEREIN, MAY IT PLEASE THIS HONOURABLE COURT TO:

GRANT the applicant's originating application for authorization to institute a class action and to obtain the status or representative against the Respondent;

AUTHORIZE the following Class action:

An action in damages against the Respondent in reparation of the harm caused by the Respondent's unlawful violation of the Class Member's right to privacy and inviolability, and its misrepresentations and

omissions regarding the privacy features of its Google Photos application.

GRANT the status of representative to Michael Homsy for the purpose of instituting the said Class action for the benefit of the following group of persons, namely:

All individuals residing in the Province of Quebec, except for Excluded Persons, who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos during the Class Period.

IDENTIFY the principal questions of law and of fact to be dealt with collectively as follows:

A. Did the Respondent breach articles 3,10, 35, 36, and/or 37, and 1457 and/or 1458 of the *CCQ*?

B. Did the Respondent breach its statutory obligations under the *PPIPS*?

C. Did the Respondent breach articles 1 and/or 5 of the *Charter*?

D. Did the Respondent breach articles 219 and 228 of the *Consumer Protection Act*?

E. Are Class Members entitled to material and/or moral damages?

F. Are Class Members entitled to punitive damages?

G. What are the amounts of the aggregate moral, material and punitive damages to be awarded to the Class?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

f. **GRANT** the applicant's action against the Respondent;

g. **DECLARE** that the Respondent:

iv. Violated its statutory obligations under the *CCQ* and the *PPIPS*;

v. Intentionally and unlawfully violated class members' rights to privacy and inviolability under the *Charter*,

vi. Violated its statutory obligations under the *Consumer Protection Act*;

h. **CONDEMN** the Respondent to pay the Class Members material, moral and punitive damages in amounts to be determined by the Court based on the evidence at trial;

i. **ORDER** collective recovery in accordance with articles 595-598 of the *CCP* for the moral and punitive damages, and individual recovery with articles 599-601 of the

CCP for the material damages;

j. **CONDEMN** the Respondent to any other remedy deemed appropriate, just, and reasonable;

THE WHOLE WITH COST, with legal costs, including the costs of all publications of notices, experts and expert reports and the attendance fees of the experts to present these reports in Court.

DECLARE that all Class Members that have not requested their exclusion from the Class in the prescribed delay to be bound by any judgment to be rendered on the class action to be instituted;

FIX the delay of exclusion at 30 days from the date of the publication of the notice to the Class Members;

ORDER the publication of a notice to the Class Members in accordance with article 579 of the *CCP*, pursuant to a further Order of the Court;

ORDER that the class action be tried in the judicial district of Montreal;

THE WHOLE with legal costs, including the costs of all publications of notices, experts and expert reports and the attendance fees of the experts to present these reports in Court.

TORONTO, January 15, 2021

John Archibald

INVESTIGATION COUNSEL PC
Co-Counsels for the Applicant
Michael Homsy
Me John Archibald
jarchibald@investigationcounsel.com
350 Bay Street, Suite 300
Toronto, ON, M5H 2S6
Phone: 416 637 3152
Fax: 416 637 3445

MONTREAL, January 15, 2021

CaLex Legal inc.

CALEX LEGAL INC.
Co-Counsels for the Applicant
Michael Homsy
Me Jean-Philippe Caron
Me Alessandra Esposito Chartrand
jpc@calex.legal
aec@calex.legal
4214 rue St-Jacques
Montréal, QC, H4C 1J4
Phone: 514 548 3023
Fax: 514 846 8844
O/R: 1349-01
BP3268

SUMMONS
(articles 145 and following C.C.P.)

Filing of a judicial application

Take notice that the applicant has filed this originating application in the office of the Superior Court in the judicial district of Montréal.

Respondent's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montréal situated at 1 rue Notre-Dame Est, Montréal, Québec within 15 days of service of this application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the applicant's lawyer or, if the applicant is not represented, to the applicant.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgement may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the applicant in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of this summons. However, in family matters or if you have no domicile, residence or establishment in Québec, it must be filed within 3 months after service; or
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Where to file the judicial application

Unless otherwise provided, the judicial application is heard in the judicial district where your domicile is located, or failing that, where your residence or the domicile you elected or agreed to with applicant is located. If it was not filed in the district where it can be heard and you want it to be transferred there, you may file an application to that effect with the court.

However, if the application pertains to an employment, consumer or insurance contract or to the exercise of a hypothecary right on the immovable serving as your main residence, it is heard in

the district where the employee's, consumer's or insured's domicile or residence is located, whether that person is the applicant or the respondent, in the district where the immovable is located or, in the case of property insurance, in the district where the loss occurred. If it was not filed in the district where it can be heard and you want it to be transferred there, you may file an application to that effect with the special clerk of that district and no contrary agreement may be urged against you.

Transfer of application to the Small Claims Division

If you qualify to act as a applicant under the rules governing the recovery of small claims, you may contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the applicant's legal costs will not exceed those prescribed for the recovery of small claims.

Convening a case management conference

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing that, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the originating application, the applicant intends to use the following exhibits:

Exhibit P-1 : Google LLC, State of California Filing ;

Exhibit P-2 : Biometrics: Principles and Legal Duties of Organizations, by the *Commission d'accès à l'information du Quebec* ;

Exhibit P-3 : Investigation report published October 28, 2020 by the *Privacy Commissioner of Canada* and *privacy commissioners in Alberta and British Columbia* ;

Exhibit P-4 : Bill C-11 ;

Exhibit P-5 : Article *Google Photos update brings facial recognition to Canadian users* ;

Exhibit P-6 : Article *How Google Photos joined the billion-user club* ;

Exhibit P-7 : Article *Updating Google Photos' storage policy to build for the future* ;

Exhibit P-8 : Article *FaceNet: A Unified Embedding for Face Recognition and Clustering* ;

Exhibit P-9 : Google Terms of service, effective date April 30, 2014 ;

Exhibit P-10 : Google Terms of service, effective date October 25, 2017 ;

Exhibit P-11 : Google Terms of service, effective date March 31, 2020 ;

Exhibit P-12 : Google Privacy policy, effective date August 19, 2015 ;

Exhibit P-13 : Google Privacy policy, effective date March 25, 2016 ;

Exhibit P-14 : Google Privacy policy, effective date May 25, 2018 ;

Exhibit P-15 : Google Privacy policy, effective date September 30, 2020 ;

Exhibit P-16 : Google Key terms ;

Exhibit P-17 : Google Our Privacy and Security Principles ;

Exhibit P-18 : Article *How Google uses pattern recognition to make sense of images* ;

Exhibit P-19 : Receipt confirming the applicant's subscription to Dropbox cloud storage as of January 14 2021 ;

These exhibits are available on request.

Notice of presentation of an application

Applications filed in the course of a proceeding and applications under Book III or V of the Code but excluding applications pertaining to family matters under article 409 and applications pertaining to securities under article 480 as well as certain applications under Book VI of the Code, including applications for judicial review, must be accompanied by a notice of presentation, not by a summons. In such circumstances, the establishment of a case protocol is not required.

NOTICE OF PRESENTATION

RECIPIENT : **GOOGLE LLC,** a legal person, duly constituted according to law, with its head office located at 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA;

Respondent

TAKE NOTICE that this application for authorization to institute a class action will be presented before the Superior Court at the Montréal courthouse, located at 1 Rue Notre-Dame Est, in the city and district of Montréal, on a date to be determined by the coordinating judge of the Class Action Division.

PLEASE ACT ACCORDINGLY.

TORONTO, January 15th 2021

John Archibald

INVESTIGATION COUNSEL PC
Co-Counsels for the Applicant
Michael Homsy
Me John Archibald
jarchibald@investigationcounsel.com
50 Bay Street, Suite 300
Toronto, ON, M5H 2S6
Phone: 416 637 3152
Fax: 416 637 3445

MONTREAL, January 15th 2021

CaLex Legal inc.

CALEX LEGAL INC.
Co-Counsels for the Applicant
Michael Homsy
Me Jean-Philippe Caron
Me Alessandra Esposito Chartrand
jpc@calex.legal
aec@calex.legal
4214 rue St-Jacques
Montréal, QC, H4C 1J4
Phone: 514 548 3023
Fax: 514 846 8844
O/R: 1349-01
BP3268

Signature Certificate

Document Ref.: 4VXRY-YD9EE-GSUOY-MG2RF

Document signed by:

Jean-Philippe Caron

Verified E-mail:
jpc@calex.legal

IP: 50.100.155.28 | Date: 15 Jan 2021 16:01:33 UTC

CaLex Legal inc.

John Archibald

E-mail:
jarchibald@investigationcounsel.com

Signed via link

IP: 208.69.14.151 | Date: 15 Jan 2021 16:39:06 UTC

John Archibald

Document completed by all parties on:
15 Jan 2021 16:39:06 UTC

Administrative information's

Matter of dispute:
CLASS ACTION

Amount: **N/A**

O/R: **1349-01**

No. 500-06-001123-211

SUPERIOR COURT OF QUEBEC
CLASS ACTION
DISTRICT OF MONTRÉAL

MICHAEL HOMSY

Applicant

c.

GOOGLE LLC.

Respondent

ORIGINATING APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION AND TO OBTAIN THE STATUS OF REPRESENTATIVE
(Articles 574 and following C.C.P.)

ORIGINAL

CaLex Legal Inc. | Investigation Counsel PC
4214 St-Jacques St. | 350 Bay St.
Montreal, QC, H4C1J4 | Toronto, ON, M5H 2S6
P: +1 514.548.3023 | 416.637.3152
F: +1 514.846.8844 | 416.637.3445
Co-Counsels for the Applicant
MICHAEL HOMSY
Me Jean-Philippe Caron | Me John Archibald
Me Alessandra Esposito Chartrand
jpc@calex.legal
aec@calex.legal
jarchibald@investigationcounsel.com
BP3268

ANNEXE 3

Pièce P-3

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia

Table of Contents

PIPEDA (Personal Information Protection and Electronic Documents Act) Report of Findings #2020-004

October 28, 2020

Overview

The Office of the Privacy Commissioner of Canada (OPC), Office of the Information and Privacy Commissioner of Alberta (OIPC AB) and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC), collectively referred to as "the Offices" commenced a joint investigation [1](#fn1), [2](#fn2) to examine whether The Cadillac Fairview Corporation Limited (CFCL) was collecting and using personal information of visitors to its Canadian malls, without valid consent, via:

i. Anonymous Video Analytics (AVA) technology installed in "wayfinding" directories; and
ii. mobile device geolocation tracking technologies.

Our findings in respect of these two issues are detailed below.

CFCL (Cadillac Fairview Corporation Limited) collected and used personal information, including sensitive biometric information, via the AVA (Anonymous Video Analytics) technology without valid consent.

The AVA (Anonymous Video Analytics) technology: (i) took temporary digital images of the faces of any individual within the field of view of the camera in the directory (retained in computer memory briefly during processing); (ii) used facial recognition software to convert those images into biometric numerical representations of the individual faces (sensitive personal information that could be used to identify individuals based on their unique facial features); and (iii) used that information to assess age range and gender.

CFCL (Cadillac Fairview Corporation Limited) represented that the numerical representations were not retained beyond processing. However, our investigation revealed that CFCL (Cadillac Fairview Corporation Limited)'s AVA (Anonymous Video Analytics) service provider had collected and stored approximately 5 million numerical representations of faces on CFCL (Cadillac Fairview Corporation Limited)'s behalf, on a decommissioned server, for no apparent purpose and with no justification.

CFCL (Cadillac Fairview Corporation Limited) explained that it collected information via AVA (Anonymous Video Analytics) for purposes of monitoring foot traffic patterns and predicting demographic information about mall visitors. We found no evidence that CFCL (Cadillac Fairview Corporation Limited) had used the biometric information, including any of the retained numerical representations, for identification purposes.

CFCL (Cadillac Fairview Corporation Limited) also retained approximately 16 hours of video recordings, some including audio, which it had captured during a calibration (or testing) phase of the technology at two malls.

CFCL (Cadillac Fairview Corporation Limited) asserted that to the extent that it required consent, such consent was obtained via its privacy policy. We found that this was inadequate. Firstly, an individual would not, while using a mall directory, reasonably expect their image to be captured and used to create a biometric representation of their face, which is sensitive personal information, or for that biometric information to be used to guess their approximate age and gender. As such, CFCL (Cadillac Fairview Corporation Limited) should have obtained express opt-in consent. Further, we reviewed CFCL (Cadillac Fairview Corporation Limited)'s privacy policy and determined that the language was overly broad, and buried in the middle of a 5,000 word document, which would not be easily accessible to individuals while they are engaging with a mall directory. We found that the privacy policy language was not sufficient to support meaningful consent for CFCL (Cadillac Fairview Corporation Limited)'s AVA (Anonymous Video Analytics) practices.

Finally, we noted that while shoppers were directed, by stickers displayed at mall entrances, to visit guest services to obtain a copy of CFCL (Cadillac Fairview Corporation Limited)'s privacy policy, when we asked a guest services employee at one of CFCL (Cadillac Fairview Corporation Limited)'s malls for that policy, they were confused by the request.

As a result of these findings, we made several recommendations. We recommended that CFCL (Cadillac Fairview Corporation Limited) either: (i) obtain meaningful express opt-in consent and allow individuals to use its mall directories without having to submit to the collection and use of their sensitive biometric information; or (ii) cease use of its AVA (Anonymous Video Analytics) technology. While CFCL (Cadillac Fairview Corporation Limited) expressly disagreed with our findings, it advised that it had ceased use of the technology in July 2018, and that it had no current plans to resume that use. CFCL (Cadillac Fairview Corporation Limited) has also, pursuant to further recommendations by our Offices, deleted the numerical representations of faces and audio/video recordings in its possession which were not required for legal purposes. It has confirmed that what information has been retained will not be used for any other purposes outside of those required for compliance with the law. CFCL (Cadillac Fairview Corporation Limited) also provided privacy-related training to guest services employees. As a result, we found the matter to be **well-founded and resolved**.

Our Offices asked CFCL (Cadillac Fairview Corporation Limited) to provide a commitment to follow our recommendations with respect to ensuring valid consent if they were to resume use of AVA (Anonymous Video Analytics) technology in the future. CFCL (Cadillac Fairview Corporation Limited) indicated that if it did resume use of the AVA (Anonymous Video Analytics) technology, it would obtain adequate consent, "in accordance with the applicable privacy legislation and consistent with the *Guidelines for obtaining meaningful consent*". However, it refused to commit to obtaining **express opt-in** consent consistent with our recommendations. We find this concerning given that CFCL (Cadillac Fairview Corporation Limited) disagreed with our analysis and interpretation of the law in this case. For example, CFCL (Cadillac Fairview Corporation Limited) continues to maintain, contrary to our findings, that they were not collecting personal information via the AVA (Anonymous Video Analytics) technology.

CFCL (Cadillac Fairview Corporation Limited) *did not* collect the location information of identifiable individuals via mobile device tracking technology in its malls, such that it did not require consent for the practice.

We found that the information collected from mobile devices of shoppers, who were not logged into Wi-Fi in CFCL (Cadillac Fairview Corporation Limited) malls, did not constitute personal information. More specifically, the hashed and randomized MAC (Media Access Control) address (device identifier), coupled with non-granular "zone" geolocation information collected using Wi-Fi triangulation, did not constitute personal information in this context, as there was not a serious possibility that this information could be linked, either alone or with other available information, with the mobile device holder.

With respect to individuals who log in to CFCL (Cadillac Fairview Corporation Limited)'s free Wi-Fi service, via a process that required them to provide personal information, we originally understood, based on the evidence gathered during our investigation, including from CFCL (Cadillac Fairview Corporation Limited) and its Wi-Fi service provider, that CFCL (Cadillac Fairview Corporation Limited) was collecting triangulated device geolocation information and linking it with identifiable device users' Wi-Fi accounts. We therefore made certain preliminary recommendations to CFCL (Cadillac Fairview Corporation Limited) with respect to the consent we would expect for this practice. However, in response to a preliminary report issued by our Offices, CFCL (Cadillac Fairview Corporation Limited) clarified, and its third-party Wi-Fi

service provider verified, that the geolocation information described above could not in any practical manner be associated with, or linked to, logged-in Wi-Fi accounts, such that it was not personal information in that context. We therefore determined the matter to be **not well-founded**.

We did note, however, that CFCL (Cadillac Fairview Corporation Limited) was seeking consent for "special location-based offers", despite the fact that it was not engaged in the practice. Further to our recommendation, CFCL (Cadillac Fairview Corporation Limited) did remove such language from its privacy policy, and added language making clear what limited location information is collected and associated with Wi-Fi accounts (i.e., only the CFCL (Cadillac Fairview Corporation Limited) property in question).

Finally, we note that CFCL (Cadillac Fairview Corporation Limited)'s third-party Wi-Fi service provider offers the option to associate triangulated "zone" information to accounts, and that CFCL (Cadillac Fairview Corporation Limited) did include, in its privacy policy, the prospect of using geolocation information to deliver location-based offers. We therefore recommended that CFCL (Cadillac Fairview Corporation Limited) commit to implementing our preliminary recommendations should it decide to activate this functionality and associate geolocation information with Wi-Fi accounts in future. Specifically, we would expect CFCL (Cadillac Fairview Corporation Limited) to: (i) support express consent for such geolocation practices via a clear and prominent notice on the Wi-Fi log-in page; and (ii) provide a clearly explained and easily accessible opt-out option. CFCL (Cadillac Fairview Corporation Limited) again refused, claiming that these recommendations were speculative.

Background

1. This report of investigation examines The Cadillac Fairview Corporation Limited's ("CFCL") compliance with Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), Alberta's' *Personal Information Protection Act* ("PIPA AB"), and British Columbia's *Personal Information Protection Act* ("PIPA BC") – referred to collectively as the "Acts".
2. CFCL is one of the largest owners, operators and developers of offices, retail and mixed-use properties, including shopping malls, in North America.
3. This joint investigation was launched in the wake of numerous media reports that raised questions and concerns about whether CFCL was collecting, using and/or disclosing personal information using facial analytics technology, via in-mall directories, without adequate consent. The technology, which CFCL referred to as Anonymous Video Analytics ("AVA") technology, [3](#fn3) was installed on digital wayfinding directories, which are effectively touch screen digital map systems that allow visitors to locate stores and find their way through CFCL shopping malls. In the context of this report, AVA technology covers all elements of the software suite and hardware elements involved in CFCL's AVA implementation.
4. Initial media reports [4](#fn4) regarding CFCL's use of AVA technology in its directories surfaced in July 2018, after an individual posted a photo [5](#fn5) on Reddit [6](#fn6) taken at CFCL's Chinook Centre in Calgary, Alberta, showing a display screen with coding language that included "FaceEncoder" and "FaceAnalyzer" – leading the media to report that CFCL was using facial recognition technologies.
5. Satisfied that reasonable grounds existed to investigate these matters, the Privacy Commissioner of Canada, Information and Privacy Commissioner for British Columbia and Information and Privacy Commissioner of Alberta each initiated investigations pursuant to s.11(2) of PIPEDA (Personal Information Protection and Electronic Documents Act), s.36(1)(a) of PIPA BC (Personal Information Protection Act (British Columbia)), and s.36(1)(a) of PIPA AB (Personal Information Protection Act (Alberta)), respectively. In August 2018, OIPC AB (Office of the Information and Privacy Commissioner of Alberta) also received a complaint about CFCL. In December 2018, the Office of the Privacy Commissioner of Canada ("OPC"), the Office of the Information & Privacy Commissioner for British Columbia ("OIPC BC"), and the Office of the Information and Privacy Commissioner of Alberta ("OIPC AB") decided to conduct the investigation jointly, at which time, the complaint received by OIPC AB (Office of the Information and Privacy Commissioner of Alberta) was put in abeyance, pending the outcome of this joint investigation.

6. In light of subsequent media reports [7](#fn7) and information obtained during the preliminary stages of the investigation into CFCL's deployment of the AVA technology, the scope of the joint investigation was expanded to determine whether CFCL obtained adequate consent for its collection, use, and disclosure of mall visitors' personal information, including geolocation and Media Access Control (MAC) [8](#fn8) address, via mobile device geolocation technologies. Further information discovered during the course of the investigation prompted us to also consider the retention of personal information obtained through the AVA technology.
7. Finally, in light of the fact that the *Commission d'accès à l'information du Québec* (the "CAI") was also examining the issue of AVA technology installed in CFCL shopping malls located in the Province of Quebec, the OPC (Office of the Privacy Commissioner of Canada), OIPC BC (Office of the Information and Privacy Commissioner of British Columbia) and OIPC AB (Office of the Information and Privacy Commissioner of Alberta) entered a collaboration arrangement with the CAI (Commission d'accès à l'information du Québec) in March 2019 in order to coordinate investigative efforts.

Methodology

8. The investigative team sought representations and records relating to the possible collection, use or disclosure of personal information by CFCL with regard to both the AVA technology and geolocation technologies. These representations were sought from CFCL directly, as well as from the following third parties: (i) Mappedin, the third party service provider of the wayfinding directories (and AVA technology therein); and (ii) Aislelabs, the third party service provider for the geolocation technologies.
9. After reviewing the initial representations from CFCL, the investigative team conducted a site visit at CFCL's headquarters in Toronto, Ontario, during which it interviewed key personnel and viewed CFCL's wayfinding directory in action, and the AVA technology therein. The investigative team also securely extracted records from the wayfinding directory for forensic analysis by the team's Technology Analysts.
10. Subsequently, the investigative team also conducted a site visit at Mappedin's headquarters, during which it interviewed key personnel, and securely extracted records for forensic analysis by the team's Technology Analysts. Further, we obtained a copy of the database containing all of the data sent by the AVA technology installed in the wayfinding directories while the technology was operational. We note that this database was stored on a decommissioned server, and was not being used for production purposes.
11. The investigation also included a visit to a CFCL property (CF (Cadillac Fairview) Eaton Centre), with the specific goal of assessing CFCL customer service staff's ability to respond to basic customer privacy requests (e.g., provision of a copy of CFCL's privacy policy).
12. Over the course of the investigation, we also considered the following material relied upon by CFCL:
    i. CFCL provided a third-party analysis report (the "Third-Party Report") produced by an Associate Professor at the Faculty of Engineering at the Bar Ilan University in Israel ("the professor") whose research relates to high computer vision, machine learning, biometrics, and signal processing;
    ii. A white paper titled *Anonymous Video Analytics (AVA) technology and privacy*, [9](#fn9) published by the Office of the Information and Privacy Commissioner of Ontario; and
    iii. A white paper entitled *Building Privacy Into Mobile Location Analytics (MLA) Through Privacy by Design*, [10](#fn10) published jointly by the Office of the Information and Privacy Commissioner of Ontario, and Aislelabs.
13. Upon completion of our investigation, we issued a preliminary report of investigation to CFCL, which set out and explained the rationale for our preliminary conclusions and identified several recommendations. We then met with CFCL to address any questions or comments they had, and to discuss our recommendations. Subsequently, in its response to our preliminary report, CFCL committed to implement a number of our recommendations which would bring it into compliance with Canadian privacy laws. CFCL also provided further submissions and factual clarifications, which led our Offices to seek further commitments to ensure that CFCL would not contravene Canadian privacy laws through the future launch or reinstitution of practices similar to those examined in our investigation. CFCL refused to provide those commitments. All of the above is detailed in this final report.

14. The investigation and findings focus on CFCL's legal obligations under the above-mentioned Acts. While this report examines the practices of certain third parties who provided services to CFCL, it does not draw any conclusions about the legal obligations of these parties, or any other organization or individual.

Issues

15. The issues in this investigation are:
    i. Whether CFCL's use of the AVA technology, via wayfinding directories, resulted in the collection, use and/or disclosure of personal information; and if yes,
        a. Whether CFCL obtained adequate consent for that collection, use and/or disclosure; and
        b. Whether CFCL retained that information for longer than necessary; and
    ii. Whether CFCL's use of mobile device geolocation tracking technologies resulted in the collection, use and/or disclosure of personal information; and if yes, whether CFCL obtained adequate consent for that collection, use and/or disclosure.

CFCL's Jurisdictional Challenge

AVA Technology

16. At the outset of our investigation, and throughout its course, CFCL objected to our jurisdiction with respect to its use of the AVA technology, on the basis that the use of the technology did not result in the collection, use, or disclosure of personal information.
17. In its representations, CFCL asserted that the information processed and gathered through the AVA technology was not personal information because it was anonymous, and in no way could it be used, alone or in combination with other information, to identify an individual. CFCL contended that all processing occurred locally and in real time, and at no time was an image, photograph or video created – except during testing and calibration, as covered at paragraph 54 of this report.
18. CFCL explained that no attempt was made to obtain a positive identification of individuals within the visible field of view of the camera, and that the digital images were not matched against a database of known individuals.
19. CFCL further represented that it was not engaged in the collection of personal information as defined by the Acts because nothing was "captured" by the AVA technology, and that "the absence of an 'identifiable individual' renders any 'capture' insufficient to qualify as collection of personal information".
20. Ultimately, after consideration of CFCL's representations, and for the reasons outlined under "Issue 1" below, we determined that CFCL was collecting personal information via its AVA technology, such that we had jurisdiction to investigate this matter.

Geolocation Technology

21. CFCL also objected to our Offices' jurisdiction with respect to its use of geolocation technologies across its properties, on the basis that MAC (Media Access Control) addresses do not constitute personal information, and that the geolocation is about a device and not about an identifiable individual.
22. In order to support its argument, CFCL drew a comparison with license plates on vehicles, and referred to the Alberta Court of Appeal's decision in *Leon's Furniture v (versus). Alberta (Information and Privacy Commissioner)*. [11](#fn11) CFCL asserted that MAC (Media Access Control) addresses are analogous to license plates:

> *"It is the mechanism that allows the vehicle to participate in the network of roads, it is visible and intended to be visible both to other vehicles and owners/operators of the roadways, and it is unique to that vehicle. Importantly, like a license plate, a MAC (Media Access Control) address is unique to a device, not an individual."*

23. In addition, CFCL further supported its position by referring to a past OPC (Office of the Privacy Commissioner of Canada) case [12](#fn12) wherein the OPC (Office of the Privacy Commissioner of Canada) held that IP (Internet Protocol) addresses [13](#fn13) can constitute personal information *if* they can be associated with or linked to an identifiable individual.
24. Our Offices considered CFCL's arguments as well as its representations, in determining whether CFCL did, in fact, collect personal information in the form of Wi-Fi triangulated geolocation data. As detailed under "Issue 2" below, our preliminary conclusion was that CFCL was collecting personal information via mobile-tracking technologies. However, subsequent to the issuance of our preliminary report, based on clarifications from CFCL and Aislelabs, we determined this not to be the case.

Issue 1: Whether CFCL's use of the AVA technology, via in-mall directories, resulted in the collection, use and/or disclosure of personal information, and if yes, whether CFCL obtained adequate consent for the collection, use and/or disclosure; and whether CFCL retained such information longer than necessary

CFCL Representations and our Investigation

Overview of CFCL's AVA Implementation

25. CFCL contracted with a third-party company, Mappedin, to provide CFCL with software and support services for interactive digital wayfinding directories, which CFCL installed in many of its retail properties across Canada. Mappedin describes itself as providing an indoor geographical information system. The organization works with nine out of ten of the largest malls in Canada, including some owned by CFCL, and claims that it seeks to help make the indoors more discoverable in stores, hospitals, campuses, and airports around the world. Additional related services under the contract with CFCL include map design, user experience development, and ongoing support and hosting.
26. The wayfinding directories all contained optical devices (i.e., cameras) behind protective glass on the periphery of the screen, such that they were not easily noticeable. The cameras were non-operational when first installed because they were not supported by underlying software. CFCL advised that AVA technology, consisting of a particular software package, was first installed by Mappedin on June 13, 2017 on a test basis, and then disabled and removed on December 1, 2017, ("Testing Period"). The AVA technology was subsequently rolled out in 12 malls across Canada (roughly 60% of directories) between May 31 2018 and July 31 2018. [14](#fn14) CFCL indicated that they considered this implementation to be a "pilot project". The AVA technology was operational in wayfinding directories in the following shopping malls:

Property	Province

Property	Province
CF (Cadillac Fairview) Market Mall	Alberta
CF (Cadillac Fairview) Chinook Centre	Alberta
CF (Cadillac Fairview) Richmond Centre	British Columbia
CF (Cadillac Fairview) Pacific Centre	British Columbia
CF (Cadillac Fairview) Polo Park	Manitoba
CF (Cadillac Fairview) Toronto Eaton Centre	Ontario
CF (Cadillac Fairview) Sherway Gardens	Ontario
CF (Cadillac Fairview) Lime Ridge	Ontario
CF (Cadillac Fairview) Fairview Mall	Ontario
CF (Cadillac Fairview) Markville Mall	Ontario
CF (Cadillac Fairview) Galeries d'Anjou	Quebec
CF (Cadillac Fairview) Carrefour Laval	Quebec

27. According to CFCL, during the initial testing and calibration period (as described in paragraph 54), and between May 2018 and July 2018, when the AVA technology was operational, the technology generated data, which was then sent for analysis by Mappedin, which provided CFCL with anonymous, aggregate insights into traffic patterns and directory use.

Further details regarding Mappedin

28. According to the latest Master Agreement (the "Agreement") between CFCL and Mappedin, dated July 20, 2017, all information provided by CFCL remained CFCL's sole and exclusive property. It further provided that all data produced under the Agreement was shared property between CFCL and Mappedin, and licensed to CFCL for use and distribution to any third party by CFCL (except under the circumstance where such third party was deemed by Mappedin as a competitor). We note that while the Agreement did mention the integration of webcams, it did not make any reference to the AVA technology. Nevertheless, based on the terms of the Agreement, we understand that CFCL remained responsible for information collected by Mappedin on its behalf.
29. In representations to our offices, Mappedin advised that it does not use the information obtained in the context of the Agreement for any purposes other than to provide the contracted services. Mappedin further stated that it does not share, and has not shared any such information with third parties.

The AVA Technology

30. In its representations to the investigative team, CFCL described the AVA technology as "facial detection software". It stated that the AVA technology assessed objects coming into the field of view of the camera in real time to determine if there was a human face present. If the underlying software detected a human face present, the software would then produce assessments of the probable gender and age range for that face. CFCL stressed in its submissions that at no time was the AVA technology capturing images or any other personal information since

the gender and age range outputs were anonymous, and that "[n]o information other than the anonymous output data is retained."

31. As noted in paragraph 12, during the course of the investigation, CFCL retained the professor to conduct a study of the AVA technology for the investigative team's consideration. The Third-Party Report was provided to us following the initial site visit. CFCL has maintained that the AVA technology did not have any facial recognition capabilities; however the report contradicts this assertion to the extent that it references the use of a software called FaceNet, which is "facial recognition" software.
32. Following our receipt of the Third-Party Report, we reached out to the professor in order to seek more information with regard to the methodology used to conduct the analysis found in the report.
33. The professor indicated that his opinion was based on the following materials provided by CFCL's external legal representatives:
    i. A "snapshot" of the AVA technology (consisting of parts of the programming code);
    ii. A copy of the "Notification of Site Visit" issued to CFCL by the OPC (Office of the Privacy Commissioner of Canada);
    iii. The Notice of Joint Investigation issued to CFCL by the OPC (Office of the Privacy Commissioner of Canada), OIPC BC (Office of the Information and Privacy Commissioner of British Columbia) and OIPC AB (Office of the Information and Privacy Commissioner of Alberta); and
    iv. A copy of a letter provided to the OPC (Office of the Privacy Commissioner of Canada) by CFCL, responding to questions posed by the investigative team in the course of the investigation.
34. In the Third-Party Report, the professor made the following conclusions:

> *"It is my opinion that the AVA software does not report any personal information of the customers. The stored gender and coarse age estimates generated by the system are anonymous and cannot be tracked back to a particular customer."*

35. Despite the conclusions of the Third-Party Report, our investigation determined that the AVA technology in question operated differently than initially represented by CFCL, and that it indeed resulted in the collection of personal information, as detailed below.
36. We established that the AVA technology performs a number of sequential steps in generating and collecting demographic information, from image input to demographic output (age and gender estimation). These steps are, as referred to in the Third-Party Report submitted by CFCL: (i) face detection; (ii) face encoding; and (iii) face tracking.
37. CFCL's initial representations stated that the AVA technology relied on an open-source software called Rude Carnie [15](#fn15) in order to generate age and gender estimations. The developers of that software describe the purpose of the software as being able to "[d]o face detection and age and gender classification on pictures".
38. After reviewing the records extracted during our site visit at CFCL's headquarters, we learned that the AVA technology employed another software [16](#fn16) named FaceNet, described as a "face recognizer". As noted in paragraph 31, this was confirmed in our subsequent review of the Third-Party Report. On the software's webpage, a research paper [17](#fn17) provides an in-depth review of the software, describing it as being a "unified system for face verification (is this the same person), recognition (who is this person) and clustering (find common people among these faces)".

Face detection and tracking

39. Our investigation confirmed that the first step undertaken by the AVA technology was facial detection. The technology was trained to detect the visual formation of one or more human faces within the field of view of the camera installed in the wayfinding directory.
40. Once the technology detected what it assessed to be a human face, it generated a bounding box around the face, and captured the image therein for conversion and processing. This "capture" resulted in an actual digital image –

or photograph – of the face being retained for a period of a few milliseconds. We do note that, save for the testing and calibration period (see paragraph 54), no persistent image was retained after this processing.

41. Our investigation further revealed that during the detection process, the technology also has the ability to, and does, differentiate faces from one another should there be more than one face in the field of view of the camera. In order to do so, the technology attributed a unique identifier, a random number, to each face detected.
42. Mappedin represented that the software was capable of assigning a unique identifier ("unique identifier") to each face present in the field of view; however, they indicated that these unique identifiers were "randomly assigned" and "non-identifying". Both Mappedin and CFCL indicated that this feature was only in place so that the AVA technology could track and differentiate individual faces within the field of view of the camera. As such, should a user exit the field of view and subsequently return, the AVA technology would assign a new random unique identifier. An example of one such unique identifier can be found in the screen capture at paragraph 53 (referenced as "id").
43. Contrary to representations from CFCL stating that only the age and gender demographic information was retained, in the course of our investigation, we discovered that Mappedin, on behalf of CFCL, collected and retained these unique identifiers in its database, along with additional information associated therewith (including, most importantly, numerical representations of individual faces captured - see paragraphs 44 & 53 of this report). When asked the purpose for such collection, Mappedin was unable to provide a response, indicating that the person responsible for programming the code no longer worked for the company.

Face encoding and embedding

44. In order for the technology to differentiate and track individual faces interacting with a wayfinding directory, the AVA technology converted and encoded the captured images, which involved the computation of a series of measurements of each face. This process generated a numerical representation, through an embedding process, of each detected face. Once this process was complete, the captured images of faces were overwritten.

Age and gender estimation

45. Our investigation confirmed that as the captured images are processed, the AVA technology estimates the probability that the face in question falls into each of eight pre-defined age groups. These are:

0-2	4-6	8-12	15-20	25-32	38-43	48-53	60-100
1	2	3	4	5	6	7	8

46. The assessment captures these probabilities in the form of numerical values. As the sample output below demonstrates, the technology made the determination that there is a significantly higher probability that the subject would fall into age group number 6 (38-43) or 7 (48-53) than any of the other groups:

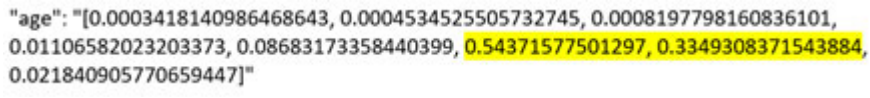


Figure 1: Sample output from the AVA technology

▶ Text version of Figure 1

47. A similar assessment process occurs for gender estimation, though the values are divided between binary options: male or female. In the sample output below, the AVA technology determined that there was a 90% probability of the face being the first binary option (male):

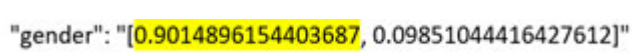


Figure 2: Sample output from the AVA technology

▶ Text version of Figure 2

48. CFCL and Mappedin both represented that the entirety of the age and gender estimation process summarized above occurs in milliseconds and that each image of a face is only stored in computer memory for the duration of that process. Our investigation confirmed that assertion. However, as noted in paragraph 50, additional information was collected and used in conjunction with the processing of the images.

Additional information sent to Mappedin

49. As previously mentioned, CFCL represented that the only information collected and retained through the deployment of the AVA technology was anonymous demographic information. It further provided that Mappedin "simply" analyzed the demographic information to provide CFCL with "anonymous, aggregate insights into traffic patterns and directory usage." However, as outlined above, our investigation discovered that Mappedin, on behalf of CFCL, collected, used and retained significantly more information than CFCL originally indicated to the investigative team.
50. Our forensic analysis of the data extracted from the wayfinding directory during the CFCL site visit revealed that in addition to the demographic information (age and gender), the AVA technology was collecting and/or generating the following information in respect of each face detection event, which was pushed to the Mappedin servers where it was retained on behalf of CFCL:
    i. A unique identifier for the wayfinding directory in which the collection occurred;
    ii. A unique identifier for the camera used for the collection;
    iii. A unique identifier for tracking and differentiating faces in the field of view;
    iv. A numerical representation of individual faces;
    v. The property in which the camera is located; and
    vi. A timestamp.
51. Following the site visit, we obtained from Mappedin the database of all information it collected, used and retained on behalf of CFCL in relation to the AVA technology. Through forensic analysis of the database, we further confirmed that CFCL, via Mappedin, had been collecting, using and retaining more than the age and gender estimation.
52. In total, for the period during which the AVA technology was operating, CFCL, via the AVA technology, collected, used and retained **5,061,324** numerical representations of faces, from an unknown number of individuals.
53. Below is a screen capture [18](#fn18) of the information collected and retained in Mappedin's database for a single face processed by the AVA technology:

Figure 3: Sample output from Mappedin's servers

▶ Text version of Figure 3

Information Collected During the Testing and Calibration Period

54. CFCL advised us that a testing and calibration exercise was undertaken before it deployed the AVA technology. Specifically, CFCL ran the calibration exercise at the CF (Cadillac Fairview) Toronto Eaton Centre and CF (Cadillac Fairview) Sherway Gardens, both located in Ontario, on April 29, May 12 and May 13, 2018 ("Calibration Period"). The Calibration Period generated sixteen one-hour videos, which Mappedin retained on behalf of CFCL.
55. We note that during our analysis of the videos, we found that in three of the sixteen videos, the audio function had been enabled, which resulted in yet another dimension to the collection, use and retention of personal information via audio recordings.

CFCL's Privacy Communications regarding AVA

56. Notwithstanding the evidence revealed through this investigation, CFCL took the position that since it was not, in its view, collecting personal information via the AVA technology, other than during the testing and calibration period, it was not required to provide notice to its customers regarding the practice.
57. We asked CFCL if it had taken any measures to inform individuals that it was conducting testing of the AVA technology, to which CFCL represented: "to the extent any personal information was collected during the testing phase, this is clearly set out CFCL's Privacy Policy…". [19](#fn19)
58. CFCL then referred to a passage in its Privacy Policy (last updated July 20, 2016) that reads as follows:

> ***2. IDENTIFYING PURPOSES***
>
> *"We collect personal information that is relevant for the purposes of providing services to our guests, service providers and clients (which includes retailers and occupants of our properties); securing our properties, websites and mobile applications; meeting our legal obligations; promoting, advertising and marketing our services and, in some cases, the products and services of our clients; and* ***researching and developing new products and techniques to improve our services****, business, our properties, websites, and mobile applications."*
>
> […]
>
> ***WHAT TYPES OF PERSONAL INFORMATION DO YOU COLLECT AND USE?***
>
> *"Some of our properties are also equipped with technologies such as ibeacons (sensors)* ***and cameras that we use to monitor foot traffic patterns and may that may [sic] assist us in predicting demographic information about our visitors during your visit to our properties****."*

59. CFCL further stated that decals on the entrance doors of all shopping malls directed guests to CFCL's Privacy Policy should they want more information on CFCL's practices. We note that, as displayed in the figure below, installed at the CF (Cadillac Fairview) Toronto Eaton Centre from May to June 2018, the only stated purposes of video recording are for "safety and security".

Figure 4: Decal on the entrance doors of the CF (Cadillac Fairview) Toronto Eaton Centre

▶ Text version of Figure 4

Analysis

Was there Collection, Use and/or Disclosure of Personal Information?

60. In our view, CFCL clearly did collect and use, via the AVA technology, personal information, as defined in the Acts, including: captured images of faces, the numerical representation assigned to each face and the assessment of age range and gender. CFCL disagrees with this finding. We also note that while CFCL collected and used numerical representations of faces suitable for facial recognition, we found no evidence that it sought to, or did, use these representations for the specific purpose of identifying individuals.
61. Subsection 2(1) of PIPEDA (Personal Information Protection and Electronic Documents Act), section 1 of PIPA BC (Personal Information Protection Act (British Columbia)) and paragraph 1(1)(k) of PIPA AB (Personal Information Protection Act (Alberta)) all define personal information as information about an identifiable individual. Courts have found in various cases that personal information must be given a broad interpretation as to give effect to the legislation's intended purpose. [20](#fn20) Courts have also found that information will be considered personal where it is reasonable to expect that a person can be identified from the information at issue when combined with information from sources otherwise available. [21](#fn21)
62. We do not accept CFCL's assertion that the AVA technology worked entirely in real-time. Rather, the captured images of individual faces coming into the field of view of the cameras were kept in memory, albeit for a very short period of time, while the technology processed these images, with the resulting information and analyses to be used thereafter.
63. The images of individual faces captured by the AVA technology through the cameras installed on the wayfinding directories are, in and of themselves, clearly personal information. Past cases have consistently found that images or photographs of individuals can and do constitute personal information under PIPEDA (Personal Information Protection and Electronic Documents Act), [22](#fn22) PIPA BC (Personal Information Protection Act (British Columbia)) [23](#fn23) and PIPA AB (Personal Information Protection Act (Alberta)). [24](#fn24) As such, while we agree that the captured images were held in memory for a very short period, that practice did represent a collection of personal information.
64. Moreover, our investigation found that the images captured by the technology were used to generate additional personal information including numerical representations, age range and gender of individual faces, which were then collected and retained for a much longer time period.

65. In particular, we are of the view that the embedding process, which results in the creation of a unique numerical representation of a particular face, constitutes a collection of biometric [25](#fn25) information, because that information is uniquely derived from a particular identifiable individual, and could be used, and is used in the context of the AVA technology in this case, to distinguish between different individuals. Based on CFCL and Mappedin's representations regarding the use of FaceNet software to detect and differentiate faces during the collection process, we have determined that these numerical representations are created by FaceNet to identify a number of facial features, which would normally enable the software to recognize specific individuals. [26](#fn26) We do note that consistent with CFCL's and Mappedin's representations, we found no evidence that either were using the technology for the purpose of identifying individuals. Nonetheless, the collection, use and retention of approximately **5 million** such numerical representations, which we view as sensitive personal information, occurred via the AVA technology.
66. As stipulated by the courts, information will be about identifiable individuals when the information in question, together with other available information would tend to or possibly identify them. [27](#fn27) "About" is also defined as being information that is not just the subject of something but also relates to or concerns the subject – such as images and/or biometric information. [28](#fn28) In that regard, previous Alberta investigations have found biometric information to be personal information. [29](#fn29) Similarly, OPC (Office of the Privacy Commissioner of Canada)'s guidance on biometrics, [30](#fn30) and past investigations, clearly affirm that biometric information is personal. [31](#fn31)
67. The England and Wales High Court of Justice recently held that biometric data, in the form of numerical representations of faces, enables the unique identification of individuals with some accuracy, which is what distinguishes it from other forms of data. [32](#fn32) As the court stated:

> *Like fingerprints and DNA, AFR [Automated Facial Recognition] technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. Taken alone or together with other recorded metadata, AFR (Automated Facial Recognition)-derived biometric data is an important source of personal information. Like fingerprints and DNA… it is information of an "**intrinsically private" character**. The fact that the biometric data is derived from a person's facial features that are "manifest in public" does not detract from this. The unique whorls and ridges on a person's fingertips are observable to the naked eye. But this does not render a fingerprint any the less a unique and precise identifier of an individual. The facial biometric identifiers too, are precise and unique* [emphasis in original document]. [33](#fn33)

68. Additionally, given that the numerical representations of individual faces were created from images already captured by the AVA technology, we are also of the view that the creation of such biometric information from the images constituted a distinct and additional collection and use of personal information regardless of the fact that the original images were not retained.
69. With respect to the White Paper referenced at paragraph 12 of this report, for the following reasons, we cannot accept CFCL's submission that the paper supports the assertion that CFCL's AVA technology did not violate PIPEDA (Personal Information Protection and Electronic Documents Act), in that no personal information was "recorded" (other than during the testing and calibration period):
    i. First, we note that the White Paper was prepared in the context of Ontario's *Freedom of Information and Protection of Privacy Act* ("FIPPA"). Subsection 2(1) of that legislation defines "personal information" as "**recorded** information about an identifiable individual", while paragraph 2(1)(a) defines "record" as "any record of information however recorded, whether in printed form, on film, by electronic means or otherwise", including "a photograph". PIPEDA (Personal Information Protection and Electronic Documents Act), PIPA BC (Personal Information Protection Act (British Columbia)) and PIPA AB (Personal Information Protection

Act (Alberta)), however, define "personal information" differently, and do not require the information to be "recorded" to constitute personal information. Therefore, compliance with these Acts cannot be resolved by reference to a report prepared in a different legislative context.

ii. Furthermore, in our view, as outlined above, personal information is "recorded" by the AVA technology in this case, since digital images must be temporarily captured in order for the technology to process them, and then further biometric and other data is derived from those images and retained. As a result, whether realized through a photo or a set of data-points, the characteristics of a face are being recorded.

70. We also do not accept CFCL's assertion that the *Morgan v (versus). Alta Flights Inc.* decision [34](#fn34) has any application to the facts presented here. That case dealt with a tape recorder that was installed by an employer to make audio recordings of its employees, but the recorder in fact failed to record audio. On that basis, the court held that because the conversation was not actually recorded, there was no collection as understood by PIPEDA (Personal Information Protection and Electronic Documents Act) in that case. However, neither the Federal Court or Federal Court of Appeal stated that personal information must, in all cases, be recorded in order to constitute a collection under PIPEDA (Personal Information Protection and Electronic Documents Act) or other private-sector privacy legislation. Furthermore, as our investigation has established, the AVA technology did in fact "record", and in our view collect, personal information in the form of images and biometrics.
71. We accept that the demographic output generated by the AVA technology, such as age and gender assessments, would not, on their own, constitute personal information for the purposes of the Acts. That said, non-identifying information can be "personal information" in context, [35](#fn35) and in this case, the demographic output was retained with other information including unique biometric information, location, and a timestamp. It is our view that the combination of this information raises a likelihood, beyond a "serious possibility", that the individual could be identified. This is the case even though we found no evidence that CFCL attempted to identify individuals from this collected personal information. It is therefore our position that the demographic output also constitutes personal information in this context.
72. As such, we cannot accept the conclusions from the Third-Party Report that the "stored gender and coarse age estimates generated by the system are anonymous". The methodology of that report was limited and failed to take into account the extensive information that had been collected and generated by CFCL, which we were able to obtain in the course of our investigation.
73. Finally, we are of the view that the collection of video and audio recordings during the calibration and testing period also constitutes a collection of personal information pursuant to the Acts.

Was there Valid Consent and Notice?

74. CFCL did not ensure valid consent and notice, for its collection and use of personal information via the AVA software, as detailed above. In coming to this determination, our Offices considered: (i) the appropriate form of consent for CFCL's practice; (ii) the meaningfulness of consent in the context at hand; and (iii) the adequacy of the notice provided by CFCL for the purposes of PIPEDA (Personal Information Protection and Electronic Documents Act), PIPA AB (Personal Information Protection Act (Alberta)) and PIPA BC (Personal Information Protection Act (British Columbia)).
75. Principle 4.3 of Schedule 1 of PIPEDA (Personal Information Protection and Electronic Documents Act) states that the **knowledge** and **consent** of the individual is required for the collection, use, or disclosure of personal information, unless these requirements are specifically exempted under section 7 of PIPEDA (Personal Information Protection and Electronic Documents Act). Principle 4.3.4 further provides that the form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. Principle 4.3.5 provides, in part, that in obtaining consent, the reasonable expectations of the individual are also relevant. Finally, Principle 4.3.6 states that the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive.

76. Similarly, section 7(1) of PIPA AB (Personal Information Protection Act (Alberta)) requires the consent of the individual for the collection, use, or disclosure of personal information, except where the Act specifies. Section 8 of PIPA AB (Personal Information Protection Act (Alberta)) sets out the various forms of consent, which include the following three possibilities:
    i. express oral or written consent;
    ii. deemed consent where it is reasonable that an individual would voluntarily provide the information for a particular purpose; and
    iii. 'opt-out' consent where the organization must provide easy-to-understand notice to the individual of the particular purposes of the collection, use or disclosure, the individual has a reasonable opportunity to decline or object, and opt-out consent is appropriate for the level of sensitivity of the personal information involved.
77. PIPA BC (Personal Information Protection Act (British Columbia)) contains similar requirements to the above. In line with section 6 of PIPA BC (Personal Information Protection Act (British Columbia)), consent for the collection, use or disclosure of personal information is required unless an exemption is specifically authorized by the Act. Subsection 7(1) of PIPA BC (Personal Information Protection Act (British Columbia)) states that an individual has not consented unless they have been given notice. In consideration of express versus implied consent, section 8(1) of PIPA BC (Personal Information Protection Act (British Columbia)) sets out the criteria under which deemed consent for the collection, use or disclosure of personal information is applicable.
78. The *Guidelines for obtaining meaningful consent* [36](#fn36) (the "Guidelines") jointly issued by the OPC (Office of the Privacy Commissioner of Canada), OIPC AB (Office of the Information and Privacy Commissioner of Alberta) and OIPC BC (Office of the Information and Privacy Commissioner of British Columbia) provide that "organizations must generally obtain *express* consent" when: (i) the information being collected, used or disclosed is sensitive; (ii) the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or (iii) the collection, use or disclosure creates a meaningful residual risk of significant harm. This is reinforced by a decision made by the Supreme Court of Canada. [37](#fn37)
79. In our view, biometric information is sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual. Within the category of biometric information, there are degrees of sensitivity. Facial biometric information is more sensitive since possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance.
80. Furthermore, mall visitors would not, in our view, reasonably expect CFCL's collection and use of their biometric information. In fact, a visitor would have no reason to expect that their image was being collected by an inconspicuous camera while searching a mall directory. Nor would such an individual expect that this image would be used to create a biometric representation in support of CFCL's commercial analytics.
81. As such, in order to comply with the Acts, and conduct its practices in accordance with the Guidelines as reinforced by the Supreme Court of Canada, CFCL should have obtained express **opt-in consent**. That consent should have been obtained **at the time of the visitor's engagement with the map**, **before *CFCL captured and processed their image*** via the AVA technology.
82. Secondly, we cannot accept CFCL's reference to its Privacy Policy as supporting meaningful consent to the collection and use of personal information via the AVA technology, whether for the video and audio recordings collected and used for calibration and testing, or for the subsequent collection and use primarily at issue.
83. Principle 4.3.2 of Schedule 1 of PIPEDA (Personal Information Protection and Electronic Documents Act) provides that an organization must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used and to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. In addition, section 6.1 of PIPEDA (Personal Information Protection and Electronic Documents Act) requires that for consent to be valid, it must be reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

84. Section 13(1) of PIPA AB (Personal Information Protection Act (Alberta)) requires that before or at the time of collecting the individual's personal information from the individual, the organization must notify the individual in writing or orally of the purposes for which the information is collected. The notice must also include the name, position, or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.
85. Section 10(1) of PIPA BC (Personal Information Protection Act (British Columbia)) requires that on or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing the purposes for the collection of the information. The organization must, upon request, also provide the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.
86. Additionally, the Guidelines provide that individuals should be made aware of all purposes for which information is collected, used or disclosed. These **purposes must be described in meaningful language, avoiding vagueness like 'service improvement'**, and **should not be buried in a Privacy Policy or terms of use** as it serves no practical purpose to individuals with limited time and energy to devote to reviewing privacy information. [emphasis added]
87. In this case, individuals would not have understood the nature of the practices in question as they had not been notified, and were otherwise unaware, that CFCL was using the AVA technology. While CFCL's Privacy Policy states that some of its properties are equipped with cameras that it uses to "monitor foot traffic patterns and [that may] assist [CFCL] in predicting demographic information" about mall visitors, and that personal information may be collected for the purpose of "researching, developing new products and techniques to improve its services", these statements would not have allowed those mall visitors to reasonably understand that while they were using a mall directory: (i) close-range video and audio recordings were being taken of them during the testing and calibration period; and/or (ii) that their faces were being detected, captured in the form of digital images, and turned into numerical representations by facial recognition software for the purposes of predicting demographic information about them, such as their age range and gender. We also note that this information is embedded approximately 2,300 words into a 5,000-word Privacy Policy, which many users will never read before their image is captured.
88. Similarly, CFCL could not rely on the decals installed on mall entrances as sufficient to ensure adequate consent under PIPEDA (Personal Information Protection and Electronic Documents Act); nor do they constitute adequate notice under PIPA AB (Personal Information Protection Act (Alberta)) or PIPA BC (Personal Information Protection Act (British Columbia)). As shown at paragraph 59 of this report, the decal only mentions that video recordings are for visitor "safety and security", and does not indicate any other purposes, such as those associated with CFCL's use of the AVA technology. Further, the link provided is a link to CFCL's website homepage, not the actual Privacy Policy. There is no indication that video recordings or cameras are used for any purpose other than "safety and security", and the wayfinding cameras are inconspicuous in comparison to the more obvious security cameras, such that there is no evident reason or prompt for visitors to search out further information about further uses in a privacy policy. These other uses, which are of a less intuitive and more questionable nature, are in fact conspicuous in their absence from the signage.
89. Moreover, the Guidelines provide that in order for consent to be considered valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner. This means that organizations must provide information about their privacy management practices in a form that is **readily accessible** [emphasis added]. We note that CFCL's wayfinding directories are physical locations, while their referenced Privacy Policy is available on their website, or at Guest Services elsewhere in the mall. Thus, the Privacy Policy is not readily accessible to individuals while they are engaging with a wayfinding map.
90. Furthermore, given that mall visitors would be unaware of the AVA technology, or even alerted that video recordings may be used for purposes beyond safety and security, they would have no reason to seek out the Privacy Policy to obtain further information, and it would not be intuitive for them to seek out an online policy to understand privacy practices in a physical shopping environment.
91. We further note that with regard to the accessibility of CFCL's Privacy Policy, we attempted, in the course of the investigation, to obtain a copy of CFCL's Privacy Policy at its Toronto Eaton Centre's Guest Service Desk. We noted that the employee seemed confused about the request, and indicated that they did not have a copy of the

Privacy Policy. It was only after returning a second time, and additional prompting, that the employee offered to print a copy of the Privacy Policy, which in fact, turned out to be CFCL's "privacy statement" as opposed to the entirety of the policy.

92. To conclude on the question of meaningfulness, it is our view that for the consent to have been meaningful, it should have been supported by a clear and conspicuous explanation of the purposes for which CFCL would capture and use individuals' personal information, as well as what information would be collected and how it would be used. CFCL provided no such explanation to wayfinding directory users and did not obtain meaningful consent for its AVA practices.

Was Personal Information Retained appropriately?

93. As noted in paragraph 52 of this report, during the course of the investigation, our Offices discovered that Mappedin retained, on CFCL's behalf, **5,061,324 numerical representations of faces** and associated information. Given that no purpose for such retention could be identified or explained, our Offices made the decision to expand the scope of the investigation to consider whether CFCL met its obligations pursuant to the provisions of the Acts pertaining to the retention of personal information.
94. As previously established, our Offices consider these numerical representations and associated information to be personal information within the meaning of the Acts. We note that principle 4.5.3 of PIPEDA (Personal Information Protection and Electronic Documents Act), section 35 of PIPA AB (Personal Information Protection Act (Alberta)) and section 35 of PIPA BC (Personal Information Protection Act (British Columbia)) all set out requirements to destroy or depersonalize any personal information when it is no longer needed to fulfill the identified purpose of its collection, or in the case of PIPA BC (Personal Information Protection Act (British Columbia)), one year subsequent to being used to make a decision. We note that when asked, Mappedin could not articulate any purpose for the collection or retention of this information on behalf of CFCL. As such, in addition to the fact that CFCL did not obtain valid consent to collect the original images, CFCL and MappedIn had no identified reason to retain these numerical representations, beyond the very brief period necessary for the AVA software to process the images. While we acknowledge Mappedin's claim that the server containing the information had been "decommissioned", this did not in our opinion, meet the requirements of the Acts, as the server was readily re-activated with all personal information accessible. In fact, we have found in breach investigations [38](#fn38) that legacy systems and "decommissioned" data, if not deleted, can quickly find their way into nefarious hands should a cyber attack occur.
95. Consequently, we find that CFCL contravened: principle 4.5.3 of Schedule 1 of PIPEDA (Personal Information Protection and Electronic Documents Act); section 35 of PIPA AB (Personal Information Protection Act (Alberta)); and section 35 of PIPA BC (Personal Information Protection Act (British Columbia)).

Recommendations

96. In our preliminary report, we recommended that if CFCL decides to pursue the use of the AVA technology in its shopping malls, it should obtain express opt-in consent, in accordance with the Acts and consistent with the *Guidelines for obtaining meaningful consent*. CFCL could, for example, undertake to implement changes to the way visitors interact with wayfinding directories by prompting a message box on the screen as soon as one or more faces are detected. The message should explain, in a simple and comprehensible way, the privacy implications associated with the AVA technology – including the collection and use of biometric information. Users should have the option to opt-in or refuse to provide consent, and should not be required to consent, as a condition to being able to use the wayfinding directory.
97. Alternatively, we recommended that CFCL cease the use of the AVA technology.
98. In addition to the above, our Offices recommended that CFCL ensure that all facial arrays (i.e., numerical representations) and associated information are deleted, as they were collected without consent and retained for no discernable purpose.
99. Finally, our Offices recommended that CFCL ensure that frontline staff are trained and kept apprised of their obligation to provide the entirety of the Privacy Policy upon request at service desks.

CFCL's Response to our Recommendations

Consent

100. CFCL (Cadillac Fairview Corporation Limited) expressly disagreed with our findings. Nevertheless, it confirmed that it had disabled its AVA software on July 31, 2018 and subsequently removed the technology from its wayfinding kiosks, and that it had no current plans to reinstall the technology.
101. CFCL also agreed to engage front-line staff in a training program that would help ensure that they are kept apprised of their obligation to provide the entirety of the Privacy Policy upon request at service desks. CFCL advised that this training was completed on July 30th 2020, and that yearly refresher training would be provided.
102. We noted that CFCL's commitments did not preclude the possibility of reimplementing its AVA program in future. We therefore asked CFCL to confirm that should it do so, it would obtain consent consistent with our Offices' recommendation, as outlined in paragraph 96 above.
103. CFCL responded that if in the future it were to pursue the use of the AVA technology in its shopping malls, it would obtain "adequate consent, in accordance with the applicable privacy legislation and consistent with the *Guidelines for obtaining meaningful consent*".
104. CFCL refused, however, to commit to obtaining consent consistent with our recommendations (i.e., to obtain express opt-in consent), asserting that our recommendation was speculative.

Retention

105. CFCL has confirmed to us that it has deleted the numerical representations and associated information and any calibration videos in its custody or under its control that are no longer necessary for legal purposes, and that no such data will be retained by CFCL or Mapped in for any other purpose. We therefore consider this aspect of the matter resolved.

Conclusion

106. To conclude, we find that CFCL engaged in the collection and use of personal information through the deployment of the AVA technology in its shopping malls without ensuring knowledge, consent or notice.
107. Consequently, we find that CFCL contravened: principles 4.3 of Schedule 1, as well as section 6.1, of PIPEDA (Personal Information Protection and Electronic Documents Act); section 7(1) and section 13(1) of PIPA AB (Personal Information Protection Act (Alberta)); and sections 6 and 10(1) of PIPA BC (Personal Information Protection Act (British Columbia)).
108. Additionally, we determined that CFCL failed to ensure the timely disposal of personal information in the form of numerical representations of faces – and related information – collected through the deployment of the AVA technology in its shopping malls.
109. Based on CFCL's commitments and facts outlined above, we accept that CFCL is currently in compliance with the Acts. We therefore consider this matter to be **well-founded and resolved** (/en/opc-actions-and-decisions/investigations/def-cf/).
110. That said, we wish to remind CFCL that regardless of whether it disagrees with our Office's findings, we expect that, should it implement AVA technology in its malls in future, it will do so in a manner that respects Canadian privacy laws, as reflected in our recommendations.

Issue 2: Whether CFCL's use of mobile device geolocation technologies resulted in the collection, use and/or disclosure of personal information, and if yes, whether CFCL obtained

adequate consent for that collection, use and/or disclosure?

CFCL's Representations and our Investigation

111. During our investigation, we asked CFCL how geolocation and MAC (Media Access Control) addresses were used, alone or in combination with other information, in order to determine whether CFCL had collected or used personal information in the context. In addition, we asked questions to determine whether CFCL obtained adequate consent for the collection and use of personal information, where required.
112. In order to corroborate the information provided to us, and better understand the practices at issue, we also sought representations from Aislelabs, a third-party service provider under contract with CFCL.

Overview of CFCL's Geolocation Implementation

113. CFCL established and maintains Wi-Fi networks at all of its retail properties in order to offer complimentary internet access to mall visitors. [39](#fn39) When a visitor with a Wi-Fi enabled device enters one of CFCL's properties, their device will be detected by a wireless access point. During communication with the access point, information is collected from the visitor's device – including its geolocation, which can be defined as information allowing for the estimation of a physical location. In other words, CFCL utilizes Wi-Fi triangulation, using signals sent from visitors' devices, to calculate their approximate position. If the visitor chooses to connect to the Wi-Fi network, they must log in and provide additional information. CFCL contracted with a third party company, Aislelabs, to analyze the information collected via its Wi-Fi access points on its behalf.
114. CFCL described two processes by which it collects information from Wi-Fi enabled devices: (i) "Anonymous Shopper Journey"; and (ii) "Logged In Shopper Journey".
    i. "Anonymous Shopper Journey": When an individual with a Wi-Fi enabled device enters a CFCL property, their MAC (Media Access Control) address is detected, and used to create a randomized unique identifier as described at paragraphs 126 and 127. If the individual does not log in, then this unique identifier and associated geolocation information is the extent of the information collected.
    ii. "Logged In Shopper Journey": If an individual chooses to log in to CFCL's Wi-Fi network with a mobile device, the device's MAC (Media Access Control) address is detected and collected as described above, and the individual is **required** to agree to CFCL's Terms and Conditions and to provide additional personal information, such as full name and email address, in exchange for access.

    Note: Subsequent to the issuance of our preliminary report, CFCL clarified, and Aislelabs verified, that when a user connects via this option, CFCL associates with the Wi-Fi account only the property at which the individual was present (e.g., CF (Cadillac Fairview) Eaton Centre), not the individual's location within that property. Aislelabs explained that while its logged-in Wi-Fi service offers the option to associate geolocation information with the account, this functionality had not yet been activated in CFCL's "Logged In Shopper Journey" implementation.
115. According to its submissions, CFCL employs geolocation technologies at all 19 of its retail properties in Canada, [40](#fn40) these being:

Property	**Province**
CF (Cadillac Fairview) Market Mall	Alberta
CF (Cadillac Fairview) Chinook Centre	Alberta
CF (Cadillac Fairview) Richmond Centre	British Columbia
CF (Cadillac Fairview) Pacific Centre	British Columbia
CF (Cadillac Fairview) Polo Park	Manitoba

Property	Province
CF (Cadillac Fairview) Champlain	New Brunswick
CF (Cadillac Fairview) Toronto Eaton Centre	Ontario
CF (Cadillac Fairview) Sherway Gardens	Ontario
CF (Cadillac Fairview) Lime Ridge	Ontario
CF (Cadillac Fairview) Fairview Mall	Ontario
CF (Cadillac Fairview) Markville Mall	Ontario
CF (Cadillac Fairview) Shops at Don Mills	Ontario
CF (Cadillac Fairview) Fairview Park	Ontario
CF (Cadillac Fairview) Masonville Place	Ontario
CF (Cadillac Fairview) Rideau Centre	Ontario
CF (Cadillac Fairview) Galeries d'Anjou	Quebec
CF (Cadillac Fairview) Carrefour Laval	Quebec
CF (Cadillac Fairview) Promenades St-Bruno	Quebec
CF (Cadillac Fairview) Fairview Pointe Claire	Quebec

116. When we asked CFCL to explain the purposes for its deployment of the geolocation technologies, it represented that it is for "counting pedestrian traffic and obtaining rough user segmentation to support CF (Cadillac Fairview) in managing pedestrian flow, and to establish the value of its properties to advertisers and merchants". In addition, CFCL uses what it described as anonymous, aggregate information to research and develop new products and techniques to improve its services for consumers and retailers.
117. CFCL stated that it did not employ geolocation "tracking" in its shopping malls, and instead indicated that the technologies it employs simply locate mobile devices to a general area or zone in its properties. CFCL took the view that it does not identify or track individuals, but mobile devices.
118. Information provided by Aislelabs indicated that their indoor geolocation capabilities are based on a Wi-Fi positioning system that can triangulate the location of devices to an area referred to as a "zone". It represented that each CFCL property consists of multiple zones. For example, the Eaton Centre was described as having 29 zones. Each zone was characterized as having several retail outlets.

Further information regarding Aislelabs

119. Aislelabs describes itself [41](#fn41) as a technology company that offers Wi-Fi location marketing and advertising, as well as an analytics platform. For CFCL, it also builds audience profiles for visitors, complete with their behavior, interests and demographics based on information collected via the Logged In Shopper Journey.
120. We note that although CFCL indicated that it does not store the information collected by Aislelabs on its behalf, the service agreement between the two parties stipulates that CFCL remains the owner of the information collected by the geolocation technologies:

> *Aislelabs acknowledges that it obtains no ownership nor proprietary rights of any nature or kind in or to the Content or Your Data or any part thereof under the terms of this Agreement. All right, title and interest in and to the foregoing (including any and all related Intellectual Property Rights, modifications and additions) thereto shall at all times remain with You.*

121. Based on the terms of this contractual agreement, we understand that CFCL remains responsible for information collected by Aislelabs on CFCL's behalf.
122. In their representations, Aislelabs confirmed that it does not use the information obtained in the context of their agreement with CFCL for any purposes other than to provide the contracted service. It was further stated that Aislelabs does not share any such information with third parties.

Anonymous Shopper Journey

123. According to the information provided by CFCL, when a Wi-Fi-enabled mobile device enters one of its properties, the MAC (Media Access Control) address of the device is detected and collected, enabling Aislelabs' software to differentiate between first time and repeat visitors, calculate the approximate location of a device inside CFCL's properties via heat maps, and capture walking paths and "dwell time".
124. Aislelabs, which collects and analyzes the information on behalf of CFCL, provides the latter with aggregated reports based on the collected information, which includes for example, statistics about the number of shoppers, repeat customers, time spent in a zone within a mall, top walking paths and heat maps representing shopper density within designated zones. CFCL is able to access those reports via a web-based dashboard.
125. Both CFCL and Aislelabs represented that this process is "anonymous" because Aislelabs' software uses a technique called hashing, which consists of using a one-way function to assign a unique identifier to the mobile device in lieu of the actual MAC (Media Access Control) address. This process is completed before the identifier is saved onto Aislelabs' database. Hashing a unique identifier offers protection against reverse engineering (or other means aimed at recovering the original value) both by the organization collecting and holding the information and by third parties. While it is theoretically possible to reverse a securely hashed value, it is highly impractical. Our Technological Analysts confirmed that based on Aislelabs' representations, they are using an algorithm currently accepted as cryptographically secure.
126. In addition to hashing the MAC (Media Access Control) addresses, Aislelabs represented that it further replaces each hashed MAC (Media Access Control) address with a random identifier, so that the hashed MAC (Media Access Control) addresses cannot be obtained from the value stored on its database. Therefore, outside of Aislelabs systems, the resulting random identifier cannot be linked to the original MAC (Media Access Control) address, providing an additional layer of depersonalization. This additional step further mitigates the risk of the original MAC (Media Access Control) address being recovered and associated to the geolocation data, by CFCL, Aislelabs or any unauthorized third party.

Logged In Shopper Journey

127. The Logged In Shopper Journey also relies on the collection of MAC (Media Access Control) addresses, which are subsequently hashed, but CFCL advised that it collects additional personal information, with consent, when a mobile device is used to connect to its complimentary Wi-Fi service. Access to CFCL's Wi-Fi requires that the visitor sign up for an account. Accordingly, CFCL collects additional information via the account creation process, such as first and last name, email address, and language preference.
128. CFCL represented that MAC (Media Access Control) addresses and geolocation information collected in the Anonymous Shopper Journey "are not, and cannot, be subsequently associated with the Logged In Shopper Journey". As such, at the time of account creation, no information is associated from previous visits made by the individual. Additionally, if a Wi-Fi user who has logged out of their account subsequently visits a CFCL property

without signing in, MAC (Media Access Control) address and geolocation data will only be collected in the form of the Anonymous Shopper Journey. Information collected during the visit will only be associated to the visitor's account if they are logged in. CFCL further asserted that the information stored in the two solutions cannot be combined in any way.

129. CFCL represented that it obtains express consent for this practice via the Terms & Conditions accessible from the login page, which incorporate the Privacy Policy explaining the practices in question.
130. More specifically, according to CFCL, when a visitor wishes to use CFCL's complimentary Wi-Fi service, they must log in using one of various available methods (i.e.: a social media account or email address), after agreeing to its Terms and Conditions ("T&C" or the "Terms"). The Terms shown on the Wi-Fi login contain the following:

> *By accessing The Cadillac Fairview Corporation Limited's Wireless Internet Service you agree to comply with the Terms of Service. If you do not accept the Terms, do not access or use the Service. The following summary of the Terms is provided for your convenience. Please read the full Terms of Service below.*
>
> *Summary*
>
> 1. *You will act lawfully, responsibly and reasonably while using the Service.*
> 2. *You assume full responsibility for your use of third party websites while using the Service.*
> 3. U*nder no circumstances will Cadillac Fairview be liable as a result of your use or inability to use the Service.*
> 4. *You agree to indemnify and hold harmless Cadillac Fairview from any all claims, relating to or arising out of your use of the Service.*
> 5. *There is no guarantee of the privacy or security of any transmission made or received through the Service.*
> 6. *As a complimentary Service, it is provided without any warranties. Cadillac Fairview does not warrant the availability or reliability of the Service.*
> 7. *Cadillac Fairview reserves the right to block certain internet websites or services, and may revoke your access to the Service at any time.*
> 8. *Cadillac Fairview may monitor your activity in connection to the Service and may disclose any information related to, as necessary.*
> 9. ***Personal information will be used as set forth in our Privacy Policy** [emphasis added]*
> 10. *The Service and the Terms may change without notice. You should check back to see the Terms in effect. Your continued use of the Service will constitute your acceptance of the Terms.*
>
> *Click **here** to accept and continue to the Wi-Fi.*
>
> *Click **here** to read the full Terms and Conditions.*

131. As highlighted in the above excerpt, the summary says that "Personal information will be used as set forth in our Privacy Policy", with an embedded link. We note that this link is actually not a link to CFCL's Privacy Policy, but instead takes individuals to a page titled "CF (Cadillac Fairview) SHOP! Privacy Statement". Individuals must scroll to the bottom of the page to view the link to CFCL's actual Privacy Policy.

132. CFCL asserted that when an individual accepts the Wi-Fi Terms, the device user provides their consent to CFCL's collection and use of their personal information, and that since "Wi-Fi Terms and Conditions expressly reference the Privacy Policy, [they] incorporate it". Should individuals choose not to accept the Terms, they would be denied use of the complimentary Wi-Fi service. While the summary does highlight provisions relating to limiting CFCL's liability, and appropriate use of the Wi-Fi service, there is no specific mention of privacy practices, beyond a link to the CF (Cadillac Fairview) SHOP! Privacy Statement.
133. In the full T&C (Terms and Conditions) document, CFCL informs users of the Wi-Fi Service (the "Service") that it may monitor, log and review users' activities in connection with their use of the Service. Further, it states that "[a]ny personal information you supply to us for the purposes of accessing the Service will be used as set forth in our Privacy Policy, which can be found at http://cfshop.ca/privacy.html and these Terms".
134. Specifically, CFCL pointed to certain sections of the Privacy Policy, including, under the section "Browser and Device Information"

> *"We may also use device information such as MAC (Media Access Control) address or other device identifiers to track foot-traffic, deliver relevant promotions and offers, customize your online experience, and to provide and manage our WIFI services."*

Another section asks "Do you use cookies, ibeacons and other similar technologies?" and says:

> *"We also use a variety of technologies to track foot traffic and mobile devices within our properties. This technology allows us to gather information on how our properties are used and also allows us (with your permission) to provide you with special location-based offers."*

135. We also noted the following, under the section "What types of personal information do you collect and use?":

> *Location Information … We use location-based information to understand how our premises are used, and to provide you with location-based offers.*

Under the heading "Do you customize promotional offers and other benefits for me?", the policy states:

> *"Please see 'What choices do I have?' for information on opting-out of these personalized promotional offers and other benefits."*

and under "What choices do I have?", the Privacy Policy says:

> *Location Information. We only collect your location information in a manner that is associated with you if you are logged into our mobile applications and authorize your device to provide us with GPS (global positioning system) information.*

Opt-Out Option

136. Aislelabs explained to our Offices that individuals have the choice to opt out of having an identifier associated to location-based analytics conducted by Aislelabs on behalf of its clients, like CFCL, by entering the MAC (Media Access Control) address of their mobile devices at an opt-out webpage. [42](#fn42) Once an individual enters the

MAC (Media Access Control) address of their device, information that may have previously been associated with that device is discarded.

137. We found no reference to, or explanation of, this opt-out option in CFCL's Privacy Policy.

Analysis

Was there Collection, Use and/or Disclosure of Personal Information?

138. First, we considered whether the information collected by CFCL using the geolocation technologies constituted personal information as defined in subsection 2(1) of PIPEDA (Personal Information Protection and Electronic Documents Act), section 1 of PIPA BC (Personal Information Protection Act (British Columbia)) and section 1(1)(k) of PIPA AB (Personal Information Protection Act (Alberta)). The Acts define personal information as information about an identifiable individual.

Anonymous Shopper Journey

139. For the reasons outlined below, we accept that CFCL is not collecting personal information in the context of the "Anonymous Shopper Journey".
140. Contrary to CFCL's position that MAC (Media Access Control) addresses are "simply not personal information", we are of the view that a MAC (Media Access Control) address **can** constitute personal information, whether it be in its original form or hashed, in certain circumstances. In our view, however, they do not constitute personal information in the circumstances of the Anonymous Shopper Journey.
141. Courts have found in various cases that personal information must be given a broad interpretation as to give effect to the legislation's intended purpose. [43](#fn43) Additionally, personal information will be considered as such if it is "about" identifiable individuals, and individuals will be considered as being identifiable when the information in question, disclosed alone or together with other publicly available information, "would tend to or possibly identify them." [44](#fn44) Moreover, "about" is also defined as being information that is not just the subject of something but also relates to or concerns the subject. [45](#fn45)
142. We note CFCL's submissions in relation to the *Leon's* [46](#fn46) case, which held that information must be identifiable and personal (i.e., directly related to the individual) in order to constitute personal information. That said, the Federal Court has more recently cautioned that information about devices and objects could still be considered personal information if it can be associated with an identifiable individual in a manner or context that reveals personal information. [47](#fn47) Furthermore, subsequent to *Leon's*, a decision [48](#fn48) made by the Alberta Court of Appeal states that "[w]here the information related to property, but also had a "personal dimension", it might sometimes properly be characterized as "personal information".
143. Information that is not, on its face, personal information, can still be considered as such if "**there is a serious possibility**" that an individual could be identified through the use of that information, alone or in combination with other available information. [49](#fn49) The application of this threshold depends on the circumstances of each case. For there to be a "serious possibility", it must be beyond mere speculation, but does not need to reach the level of "more likely than not". [50](#fn50)
144. The OPC (Office of the Privacy Commissioner of Canada) has expressed its view in a number of previous cases that device identifiers can constitute personal information, and be about an identifiable individual. For example, in a 2013 investigation into WhatsApp, [51](#fn51) the OPC (Office of the Privacy Commissioner of Canada) found that unique identifiers, user's device identifier information, mobile subscriber ID, mobile country code, and mobile network code could constitute personal information, since the information, alone or in combination with other information, could render a specific individual identifiable. The OIPC BC (Office of the Information and Privacy Commissioner of British Columbia) has also issued investigation reports that cite device identifiers as a form of personal information. For example, a 2019 report on medical clinics found that clinics should be notifying individuals before collecting personal information online, including device identifiers, and recommended that

device identifiers and other personal information collected, used, or disclosed online should be detailed in privacy policies. [52](#fn52)

145. A MAC (Media Access Control) address, depending on the context, can be personal information, for example when combined with other available information. In the case of the Anonymous Shopper Journey, the only information associated with the hashed MAC (Media Access Control) address is general and imprecise geolocation information limited to CFCL malls and their immediate surroundings. This information is not, in our view, sufficient to allow an individual to be identified as it does not contain the geographic scope or level of detail required to extrapolate identifying information such as residence, routine or specific place of employment. Furthermore, the hashing and randomization of the MAC (Media Access Control) address would render it practically infeasible to use the MAC (Media Access Control) address to link other available information about the mobile device user, such that we accept that there is not a serious possibility that the MAC (Media Access Control) address, or associated geolocation information, could be linked to that user.
146. We therefore accept that CFCL is not collecting, using or disclosing personal information in the specific context of the Anonymous Shopper Journey, as understood by this investigation.

Logged In Shopper Journey

147. As noted above, CFCL acknowledged that for its Logged In Shopper Journey, it does collect personal information via login, such as email addresses and other personal information that is provided depending on the login mechanism. In particular, CFCL represented that when visitors opt to sign into Wi-Fi using a social media account, it will collect other information associated with the account. This information is then associated to the Logged In Shopper Journey Account. It is our view that the MAC (Media Access Control) addresses and any geolocation information collected while the user is logged in would become personal information due to their association with a user account, and thus an identifiable individual.
148. Based on the new information provided to our Offices by CFCL and Aislelabs in response to our preliminary report, we now understand and accept that CFCL does not, and cannot practically, associate geolocation information derived via Wi-Fi triangulation, the subject of our investigation, with the personal information of logged-in shoppers. While theoretically, there exist methods by which CFCL could, via Aislelabs, make such an association, MAC (Media Access Control) address hashing and database separation render linking impractical.
149. Contractual and code restrictions exist. While Aislelabs may have the technical capability to link geolocation data on CFCL's WiFi network, the company would be precluded from doing so pursuant to both their contract with CFCL and the Mobile Location Analytics Code of Conduct to which they have confirmed their strict adherence. We have no evidence that Aislelabs ever attempted to make such a link, and in our view, the information in question – an approximate location of visitors within the confines of malls – would not be of justifiable value to breach contractual obligations and codes of conduct.
150. Our Offices have not considered whether CFCL obtained valid consent for information obtained from third-party social media accounts via log-in through the single sign-on process, which is outside the scope of this investigation.

Was there Valid Consent and Notice for collection of MAC (Media Access Control) Address and geolocation information?

151. Given our conclusion that CFCL is not collecting personal information via its Anonymous Shopper Journey, we accept that it did not require consent to collect that information.
152. With respect to the Logged In shopper Journey, when we issued our preliminary report, we understood that CFCL was associating geolocation information derived via Wi-Fi triangulation to the accounts of individuals using CFCL Wi-Fi. As such, we conducted a preliminary analysis with respect to the adequacy of CFCL's consent for that practice. We have now learned via CFCL's response to our preliminary report, that it was *not* associating, or linking, such geolocation information about individuals using the Wi-Fi service. [53](#fn53) While CFCL was, concurrent with the Logged In Shopper Journey, collecting triangulated location information about Wi-Fi enabled devices via the Anonymous Shopper Journey, we determined that this was not personal information in that

context. Furthermore, CFCL was not associating, and could not practically associate or link that information to personal information collected about Wi-Fi users.

153. We note, however, that Aislelabs' logged-in Wi-Fi service offers the *option* to associate triangulated "zone" information to accounts, and that CFCL did include, in its privacy policy, the assertion of using geolocation information to deliver location-based offers (see paragraph 135). We have, therefore, included our analysis with respect to the association of geolocation data with Wi-Fi accounts below, to explain our Offices' expectations should CFCL decide to activate this functionality in the future.

Meaningfulness

154. Principle 4.3 of Schedule 1 of PIPEDA (Personal Information Protection and Electronic Documents Act) states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information. Principle 4.3.2 of PIPEDA (Personal Information Protection and Electronic Documents Act) further provides that an organization must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used and that to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Section 6.1 of PIPEDA (Personal Information Protection and Electronic Documents Act) further clarifies that for consent to be valid, it must be reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.
155. Similarly, section 7(1)(a) of PIPA AB (Personal Information Protection Act (Alberta)) states that, except where otherwise authorized in the Act, "[…] an organization shall not, with respect to personal information about an individual […] collect that information unless the individual consents to the collection of that information". Section 13(1) of PIPA AB (Personal Information Protection Act (Alberta)) further requires that before or at the time of collecting the individual's personal information from the individual, the organization must notify the individual in writing or orally of the purposes for which the information is collected. The notice must also include the name, position, or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.
156. In the same vein, subsection 7(1) of PIPA BC (Personal Information Protection Act (British Columbia)) states that an individual has not consented unless they have been given notice. In some cases, notice is not required if the purpose for the collection, use or disclosure is "obvious" and the individual volunteers their information for that purpose. Section 10(1) of PIPA BC (Personal Information Protection Act (British Columbia)) further provides that on or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing the purposes for the collection of the information. The organization must, upon request, also provide the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.
157. Further to the above, the Guidelines provide that individuals should be made aware of **all** purposes for which information is collected, used or disclosed. These purposes must be described in meaningful language, avoiding vagueness like 'service improvement', and **should not be buried in a privacy policy or terms of use as it serves no practical purpose to individuals with limited time and energy to devote to reviewing privacy information**.
158. The Guidelines also provide that "to receive meaningful consent, organizations must allow individuals to quickly review key elements impacting their privacy decisions **right up front as they are considering using the service or product on offer…**" and that "organizations should **in particular highlight any purposes that would not be obvious to the individual and/or reasonably expected based on the context**" [emphasis added].
159. We note that the summary of the Terms & Conditions for accessing CFCL's Wi-Fi service includes 10 specific points, only one of which relates to privacy, and then only to the extent of saying "Personal information will be used as set forth in our Privacy Policy". The summary does not speak, even at a high level, about what personal information will be collected, nor the purpose(s) for which that information will be used. To find this information, individuals must click the hyperlink to access a Privacy Statement, and then find the link to CFCL's Privacy Policy at the bottom of that page. Many users will not, before logging in, or ever, read that 5,000 word document.

160. Consent is only valid or meaningful where individuals understand what they are consenting to. As such, in our view, should CFCL decide, in future, to collect and use triangulated or more precise geolocation information of Wi-Fi users (for example to deliver location based offers as previously stated in their Privacy Policy), CFCL would need to ensure that prospective users are made aware of this practice via a prominent notice on the log-in page before they "Click here to accept and continue to the Wi-Fi", and a clear and detailed explanation of the practice in its Privacy Policy.
161. Finally, we note that CFCL does not currently use geolocation information to deliver "special location-based offers", contrary to what it stated in its Privacy Policy. In our view, CFCL cannot meaningfully explain the manner in which it would use or disclose personal information to achieve these purposes, when it does not in fact engage in such a practice. As such, in our view, it should not be seeking such consent at this time.

Choice

162. The Acts provide that individuals shall not be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide a product or service. [54](#fn54)
163. The Guidelines further explain that for a collection, use, or disclosure to be a valid condition of service, it must be **integral** to the provision of that product or service and that where it is not, individuals must be given a choice. Purposes integral to the provision of the service should be distinguished from those that are not, and any available options must be explained clearly and made easily accessible.
164. CFCL advertises complimentary Wi-Fi as a service to entice potential shoppers to spend time at its malls. In our view, CFCL benefits from the provision of this service through the potential for increased mall traffic, even without the collection of geolocation data. While we recognize the legitimate business benefits that CFCL could potentially gain from the collection, use and disclosure of personal information via geolocation technologies and related analytics, geolocation tracking would not be integral to providing Wi-Fi services. As such, CFCL should provide individuals with the ability to opt-out should it decide to collect and associate triangulated, or more precise geolocation data with logged-in Wi-Fi accounts in the future.

Preliminary Recommendations

165. In our preliminary report, we recommended that CFCL take the following measures to ensure meaningful consent for its use of MAC (Media Access Control) address and geolocation information of individuals accessing its logged in Wi-Fi service:
    i. provide clear and prominent language, for example on the Wi-Fi log-in page, highlighting its geolocation tracking practices, the purposes for which it will use that information and how users can opt-out of the practice;
    ii. provide individuals with an easily accessible and conspicuous opt-out option for CFCL's association of their MAC (Media Access Control) address and geolocation information to accounts;
    iii. include in its privacy policy a clear explanation that geolocation tracking is not integral to the provision of its Wi-Fi service, and explaining how individuals can opt out of the practice; and
    iv. cease seeking consent for the use of geolocation and MAC (Media Access Control) address for purposes of delivering "special location-based offers" until such time as CFCL plans to engage in that practice, and is therefore able to meaningfully explain how it will use that information for such purposes.

CFCL's Response to our Recommendations

166. As outlined above, in response to our preliminary report, CFCL provided new information to our Offices confirming that it did **not** associate zone-based geolocation information to individual Wi-Fi accounts.
167. We note, however, the potential for zone-based geolocation information to be associated to the Logged In Shopper Journey using Aislelabs service (functionality that was not included in CFCL's current Wi-Fi

implementation), and the fact that CFCL's Privacy Policy had asserted the use of geolocation information to provide "special location-based offers".

168. We therefore asked that CFCL commit to follow the recommendations set out in paragraph 165 (i through iii) should it decide to activate the association of geolocation data with logged in Wi-Fi accounts in the future.
169. CFCL refused to make this commitment, asserting that our recommendations were speculative.
170. CFCL did, however, commit to cease seeking consent for the use of geolocation and MAC (Media Access Control) address for purposes of delivering "special location-based offers", a practice in which it did not engage, and to clarify that only the name of the CFCL property at which individuals connect, and not more granular location information, is associated with Wi-Fi accounts. In response to our preliminary report, CFCL has amended the language in its Privacy Policy accordingly.

Conclusion

171. On the issue of consent for collection, use and disclosure of geolocation, we find that CFCL did not collect personal information in the context of the Anonymous Shopper Journey, and did not collect triangulated geolocation information in the context of the Logged In Shopper Journey. We therefore conclude that the matter is **not well-founded** (/en/opc-actions-and-decisions/investigations/def-cf/).
172. That said, we wish to remind CFCL of our expectation that should it associate zone-based or more granular geolocation information to Wi-Fi accounts in its malls in the future, it would do so in a manner that complies with Canadian privacy laws, as reflected in our preliminary recommendations.

Footnotes

1 Throughout this report the terms "we" and "our" are used frequently. When used outside of the context of a quoted document, these terms refer to the collective of the OPC (Office of the Privacy Commissioner of Canada), OIPC AB (Office of the Information and Privacy Commissioner of Alberta) and OIPC BC (Office of the Information and Privacy Commissioner of British Columbia).

2 The three Offices subsequently entered into an information sharing arrangement with the Commission d'accès à l'information du Québec ("CAI") in March 2019 as it had also initiated an investigation into CFCL (Cadillac Fairview Corporation Limited)'s use of AVA technology, though the CAI (Commission d'accès à l'information du Québec) continued its investigation independently.

3 AVA technology generally refers to software designed to gather metrics about digital signage audience engagement. As described by the Ontario Information and Privacy Commissioner in a White Paper on AVA software, it generally operates by scanning "real-time feeds from video cameras utilizing pattern detection algorithms to identify shoppers anonymously for the purpose of creating aggregate reports".

4 Sarah Rieger, "At least two malls are using facial recognition to track shoppers ages and genders without telling," *CBC*, Jul. 26, 2018.

5 Facial Recognition Tech at Chinook?

6 Reddit is an American social news aggregation, web content rating, and discussion website. Registered members submit content to the site such as links, text posts, and images, which are then voted up or down by other members (Wikipedia).

7 Anis Heydari, "Cellphone tracking has been used in at least 1 Canadian mall, former employee says", *CBC*, August 8, 2018.

8 Media Access Control address is a 48-bit identification number embedded by manufacturers on every device's network interface controller. The MAC (Media Access Control) address uniquely identifies each device on a network.

9 White Paper: Anonymous Video Analytics (AVA) technology and privacy.

10 Building Privacy into Mobile Location Analytics (MLA) *Through Privacy by Design*.

11 2011 ABCA 94 [*Leon's*].

12 PIPEDA (Personal Information Protection and Electronic Documents Act) Report of Findings #2009-010

13 An Internet Protocol address is a numerical label assigned to a device when it connects to a network. The IP (Internet Protocol) address identifies the device and routes its network traffic.

14 While CFCL (Cadillac Fairview Corporation Limited) represented that it ceased use of the AVA technology on July 31 2018, we note that in the course of our investigation we identified information collected from AVA on Mappedin's servers bearing timestamps up to August 03 2018.

15 Rude Carnie: Age and Gender Deep Learning with TensorFlow.

16 Face Recognition using TensorFlow.

17 Florian Schroff, Dmitry Kalenichenko, James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering (2015).

18 Portions of data have been redacted for anonymization purposes, namely: the kiosk and camera identifier pointing to a specific location, authorization code, and some numerical facial representation values (which are in the same format as the values above and below the redaction). Highlighting added for ease of reference.

19 The CFCL (Cadillac Fairview Corporation Limited) Privacy Policy in effect during this investigation was available on this page. An archived copy of this Privacy Policy can be found here.

20 Dagg v (versus). Canada (Minister of Finance), [1997] 2 S.C.R. 403, dissenting, at para 68; Canada (Information Commissioner) v (versus). Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157.

21 Canada (Information Commissioner) v (versus). Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157; Girao v (versus). Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 para 32.

22 *See, e.g.* PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary 2002-53; PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary 2008-392; PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary 2002-89; PIPEDA (Personal Information Protection and Electronic Documents Act) Report of Findings 2013-016; PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary 2008-396.

23 *See, e.g.* Order P09-02 from the OIPC BC (Office of the Information and Privacy Commissioner of British Columbia).

24 *See, e.g.* Orders P2009-013 and P2009-014 from OIPC AB (Office of the Information and Privacy Commissioner of Alberta).

25 As stated on OPC (Office of the Privacy Commissioner of Canada) webpage resource, "Data at Your Fingertips Biometrics and the Challenges to Privacy":

> Originally, the word "biometrics" meant applying mathematical measurements to biology. Nowadays, the term refers to a range of techniques, devices and systems that enable machines to recognize individuals, or confirm or authenticate their identities.
>
> Such systems measure and analyze people's physical and behavioural attributes, such as facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, structures of the eye (iris or retina), or gait.

26 Florian Schroff, Dmitry Kalenichenko, James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering (2015).

27 Gordon v (versus). Canada (Health), 2008 FC 258 ; Girao v (versus). Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 para 32.

28 Canada (Information Commissioner) v (versus). Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157.

29 *See, e.g.* Investigation reports F2008-IR-001 and P2008-IR-005.

30 OPC (Office of the Privacy Commissioner of Canada), "Data at Your Fingertips Biometrics and the Challenges to Privacy", (2011).

31 *See, e.g.* PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary #2010-007, PIPEDA (Personal Information Protection and Electronic Documents Act) Case Summary #2004-281.

32 *R (Bridges) v (versus). CCSWP and SSHD*, [2019] EWHC 2341 (Admin) [UK Decision].

33 *Ibid.* at para. 57.

34 Morgan v (versus). Alta Flights Inc. (2006) FCA 121, affirming (2005) FC 421

35 Gordon v (versus). Canada (Health), 2008 FC 258 ; *See e.g,* Order P-12-01 from the Office of the Information and Privacy Commissioner for British Columbia.

36 Guidelines for obtaining meaningful consent (2018).

37 *Royal Bank of Canada v (versus). Trang*, 2016 SCC 50 paras 23 & 34

38 See e.g., Investigation into Equifax Inc. And Equifax Canada Co.'s compliance with PIPEDA (Personal Information Protection and Electronic Documents Act) in light of the 2017 breach of personal information.

39 As of February 14, 2019.

40 As of February 14, 2019.

41 Aislelabs, About Us.

42 This option is made available via a website, which allows for individuals to enter their MAC (Media Access Control) address in order to opt out of Aislelabs' Mobile Location Analytics, and that of other companies. The website is described as a project owned by the Future of Privacy Forum, a non-profit organization self-described as "advancing principled data practices in support of emerging technologies".

43 *Dagg v (versus). Canada* (Minister of Finance), [1997] 2 S.C.R. 403, dissenting, at para 68; Canada (Information Commissioner) v (versus). Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157.

44 *Girao v (versus). Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070 para 32.

45 *Canada (Information Commissioner) v (versus). Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII)

46 2011 ABCA 94 [*Leon's*].

47 *Canada (Information Commissioner) v (versus). Canada (Minister of Public Safety and Emergency Preparedness)*, 2019 FC 1279.

48 *Edmonton (City), v (versus). Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 at para 25, upholding in part 2015 ABQB 246

49 *Ibid* at para 34.

50 *Ibid* at para 53.

51 *See e.g.*, Investigation into the personal information handling practices of WhatsApp Inc; Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising; Employee text messages intercepted without authorization at the Warkworth Institution.

52 *See e.g.*, OIPC BC (Office of the Information and Privacy Commissioner of British Columbia). Audit & Compliance Report P19-01: Compliance Review of Medical Clinics.

53 While CFCL (Cadillac Fairview Corporation Limited) does collect very limited “location” information for logged-in users – i.e., the mall at which the individual has logged in to the Wi-Fi - this is not Wi-Fi-triangulated geolocation information, and is outside the scope of our investigation. That said, we note that as per paragraph 170, CFCL (Cadillac Fairview Corporation Limited) has now added language in its privacy statement to clarify that only the name of the CFCL (Cadillac Fairview Corporation Limited) property at which individuals connect, and *not* more granular location information, is associated with Wi-Fi accounts.

54 Principle 4.3.3 of PIPEDA (Personal Information Protection and Electronic Documents Act) stipulates that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

Section 7(2) of PIPA AB (Personal Information Protection Act (Alberta)) states that an organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

Section 7(2) of PIPA BC (Personal Information Protection Act (British Columbia)) provides that an organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.

Date modified:

2020-10-29

ANNEXE 4

FaceNet: A Unified Embedding for Face Recognition and Clustering

Florian Schroff
fschroff@google.com
Google Inc.

Dmitry Kalenichenko
dkalenichenko@google.com
Google Inc.

James Philbin
jphilbin@google.com
Google Inc.

Abstract

Despite significant recent advances in the field of face recognition [10, 14, 15, 17], implementing face verification and recognition efficiently at scale presents serious challenges to current approaches. In this paper we present a system, called FaceNet, that directly learns a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity. Once this space has been produced, tasks such as face recognition, verification and clustering can be easily implemented using standard techniques with FaceNet embeddings as feature vectors.

Our method uses a deep convolutional network trained to directly optimize the embedding itself, rather than an intermediate bottleneck layer as in previous deep learning approaches. To train, we use triplets of roughly aligned matching / non-matching face patches generated using a novel online triplet mining method. The benefit of our approach is much greater representational efficiency: we achieve state-of-the-art face recognition performance using only 128-bytes per face.

On the widely used Labeled Faces in the Wild (LFW) dataset, our system achieves a new record accuracy of ***99.63%****. On YouTube Faces DB it achieves* ***95.12%****. Our system cuts the error rate in comparison to the best published result [15] by 30% on both datasets.*

We also introduce the concept of harmonic *embeddings, and a* harmonic *triplet loss, which describe different versions of face embeddings (produced by different networks) that are compatible to each other and allow for direct comparison between each other.*

1. Introduction

In this paper we present a unified system for face verification (is this the same person), recognition (who is this person) and clustering (find common people among these faces). Our method is based on learning a Euclidean embedding per image using a deep convolutional network. The network is trained such that the squared L2 distances in the embedding space directly correspond to face similarity:

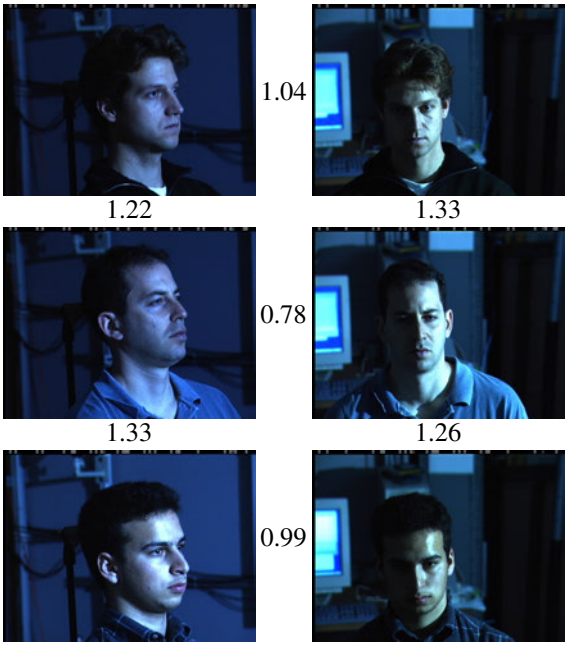


Figure 1. **Illumination and Pose invariance.** Pose and illumination have been a long standing problem in face recognition. This figure shows the output distances of FaceNet between pairs of faces of the same and a different person in different pose and illumination combinations. A distance of 0.0 means the faces are identical, 4.0 corresponds to the opposite spectrum, two different identities. You can see that a threshold of 1.1 would classify every pair correctly.

faces of the same person have small distances and faces of distinct people have large distances.

Once this embedding has been produced, then the aforementioned tasks become straight-forward: face verification simply involves thresholding the distance between the two embeddings; recognition becomes a k-NN classification problem; and clustering can be achieved using off-the-shelf techniques such as k-means or agglomerative clustering.

Previous face recognition approaches based on deep networks use a classification layer [15, 17] trained over a set of known face identities and then take an intermediate bottle-

neck layer as a representation used to generalize recognition beyond the set of identities used in training. The downsides of this approach are its indirectness and its inefficiency: one has to hope that the bottleneck representation generalizes well to new faces; and by using a bottleneck layer the representation size per face is usually very large (1000s of dimensions). Some recent work [15] has reduced this dimensionality using PCA, but this is a linear transformation that can be easily learnt in one layer of the network.

In contrast to these approaches, FaceNet directly trains its output to be a compact 128-D embedding using a triplet-based loss function based on LMNN [19]. Our triplets consist of two matching face thumbnails and a non-matching face thumbnail and the loss aims to separate the positive pair from the negative by a distance margin. The thumbnails are tight crops of the face area, no 2D or 3D alignment, other than scale and translation is performed.

Choosing which triplets to use turns out to be very important for achieving good performance and, inspired by curriculum learning [1], we present a novel online negative exemplar mining strategy which ensures consistently increasing difficulty of triplets as the network trains. To improve clustering accuracy, we also explore hard-positive mining techniques which encourage spherical clusters for the embeddings of a single person.

As an illustration of the incredible variability that our method can handle see Figure 1. Shown are image pairs from PIE [13] that previously were considered to be very difficult for face verification systems.

An overview of the rest of the paper is as follows: in section 2 we review the literature in this area; section 3.1 defines the triplet loss and section 3.2 describes our novel triplet selection and training procedure; in section 3.3 we describe the model architecture used. Finally in section 4 and 5 we present some quantitative results of our embeddings and also qualitatively explore some clustering results.

2. Related Work

Similarly to other recent works which employ deep networks [15, 17], our approach is a purely data driven method which learns its representation directly from the pixels of the face. Rather than using engineered features, we use a large dataset of labelled faces to attain the appropriate invariances to pose, illumination, and other variational conditions.

In this paper we explore two different deep network architectures that have been recently used to great success in the computer vision community. Both are deep convolutional networks [8, 11]. The first architecture is based on the Zeiler&Fergus [22] model which consists of multiple interleaved layers of convolutions, non-linear activations, local response normalizations, and max pooling layers. We additionally add several $1\times1\times d$ convolution layers inspired by the work of [9]. The second architecture is based on the *Inception* model of Szegedy *et al*. which was recently used as the winning approach for ImageNet 2014 [16]. These networks use mixed layers that run several different convolutional and pooling layers in parallel and concatenate their responses. We have found that these models can reduce the number of parameters by up to 20 times and have the potential to reduce the number of FLOPS required for comparable performance.

There is a vast corpus of face verification and recognition works. Reviewing it is out of the scope of this paper so we will only briefly discuss the most relevant recent work.

The works of [15, 17, 23] all employ a complex system of multiple stages, that combines the output of a deep convolutional network with PCA for dimensionality reduction and an SVM for classification.

Zhenyao *et al*. [23] employ a deep network to "warp" faces into a canonical frontal view and then learn CNN that classifies each face as belonging to a known identity. For face verification, PCA on the network output in conjunction with an ensemble of SVMs is used.

Taigman *et al*. [17] propose a multi-stage approach that aligns faces to a general 3D shape model. A multi-class network is trained to perform the face recognition task on over four thousand identities. The authors also experimented with a so called Siamese network where they directly optimize the L_1-distance between two face features. Their best performance on LFW (97.35%) stems from an ensemble of three networks using different alignments and color channels. The predicted distances (non-linear SVM predictions based on the χ^2 kernel) of those networks are combined using a non-linear SVM.

Sun *et al*. [14, 15] propose a compact and therefore relatively cheap to compute network. They use an ensemble of 25 of these network, each operating on a different face patch. For their final performance on LFW (99.47% [15]) the authors combine 50 responses (regular and flipped). Both PCA and a Joint Bayesian model [2] that effectively correspond to a linear transform in the embedding space are employed. Their method does not require explicit 2D/3D alignment. The networks are trained by using a combination of classification and verification loss. The verification loss is similar to the triplet loss we employ [12, 19], in that it minimizes the L_2-distance between faces of the same identity and enforces a margin between the distance of faces of different identities. The main difference is that only pairs of images are compared, whereas the triplet loss encourages a relative distance constraint.

A similar loss to the one used here was explored in Wang *et al*. [18] for ranking images by semantic and visual similarity.

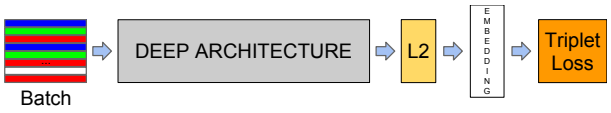


Figure 2. **Model structure.** Our network consists of a batch input layer and a deep CNN followed by L_2 normalization, which results in the face embedding. This is followed by the triplet loss during training.

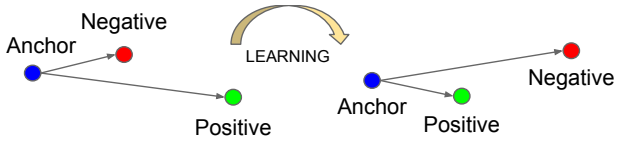


Figure 3. The **Triplet Loss** minimizes the distance between an *anchor* and a *positive*, both of which have the same identity, and maximizes the distance between the *anchor* and a *negative* of a different identity.

3. Method

FaceNet uses a deep convolutional network. We discuss two different core architectures: The Zeiler&Fergus [22] style networks and the recent Inception [16] type networks. The details of these networks are described in section 3.3.

Given the model details, and treating it as a black box (see Figure 2), the most important part of our approach lies in the end-to-end learning of the whole system. To this end we employ the triplet loss that directly reflects what we want to achieve in face verification, recognition and clustering. Namely, we strive for an embedding $f(x)$, from an image x into a feature space $\mathbb{R}^d$, such that the squared distance between *all* faces, independent of imaging conditions, of the same identity is small, whereas the squared distance between a pair of face images from different identities is large.

Although we did not directly compare to other losses, *e.g.* the one using pairs of positives and negatives, as used in [14] Eq. (2), we believe that the triplet loss is more suitable for face verification. The motivation is that the loss from [14] encourages all faces of one identity to be projected onto a single point in the embedding space. The triplet loss, however, tries to enforce a margin between each pair of faces from one person to all other faces. This allows the faces for one identity to live on a manifold, while still enforcing the distance and thus discriminability to other identities.

The following section describes this triplet loss and how it can be learned efficiently at scale.

3.1. Triplet Loss

The embedding is represented by $f(x) \in \mathbb{R}^d$. It embeds an image x into a d-dimensional Euclidean space. Additionally, we constrain this embedding to live on the d-dimensional hypersphere, *i.e.* $\|f(x)\|_2 = 1$. This loss is motivated in [19] in the context of nearest-neighbor classification. Here we want to ensure that an image x_i^a (*anchor*) of a specific person is closer to all other images x_i^p (*positive*) of the same person than it is to any image x_i^n (*negative*) of any other person. This is visualized in Figure 3.

Thus we want,

$$\|f(x_i^a) - f(x_i^p)\|_2^2 + \alpha < \|f(x_i^a) - f(x_i^n)\|_2^2 \,, \tag{1}$$

$$\forall \left(f(x_i^a), f(x_i^p), f(x_i^n)\right) \in \mathcal{T} \,. \tag{2}$$

where α is a margin that is enforced between positive and negative pairs. $\mathcal{T}$ is the set of all possible triplets in the training set and has cardinality N.

The loss that is being minimized is then $L =$

$$\sum_i^N \left[\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha\right]_+ \,. \tag{3}$$

Generating all possible triplets would result in many triplets that are easily satisfied (*i.e.* fulfill the constraint in Eq. (1)). These triplets would not contribute to the training and result in slower convergence, as they would still be passed through the network. It is crucial to select hard triplets, that are active and can therefore contribute to improving the model. The following section talks about the different approaches we use for the triplet selection.

3.2. Triplet Selection

In order to ensure fast convergence it is crucial to select triplets that violate the triplet constraint in Eq. (1). This means that, given x_i^a, we want to select an x_i^p (*hard positive*) such that $\operatorname{argmax}_{x_i^p} \|f(x_i^a) - f(x_i^p)\|_2^2$ and similarly x_i^n (*hard negative*) such that $\operatorname{argmin}_{x_i^n} \|f(x_i^a) - f(x_i^n)\|_2^2$.

It is infeasible to compute the argmin and argmax across the whole training set. Additionally, it might lead to poor training, as mislabelled and poorly imaged faces would dominate the hard positives and negatives. There are two obvious choices that avoid this issue:

- Generate triplets offline every n steps, using the most recent network checkpoint and computing the argmin and argmax on a subset of the data.
- Generate triplets online. This can be done by selecting the hard positive/negative exemplars from within a mini-batch.

Here, we focus on the online generation and use large mini-batches in the order of a few thousand exemplars and only compute the argmin and argmax within a mini-batch.

To have a meaningful representation of the anchor-positive distances, it needs to be ensured that a minimal number of exemplars of any one identity is present in each

mini-batch. In our experiments we sample the training data such that around 40 faces are selected per identity per mini-batch. Additionally, randomly sampled negative faces are added to each mini-batch.

Instead of picking the hardest positive, we use all anchor-positive pairs in a mini-batch while still selecting the hard negatives. We don't have a side-by-side comparison of hard anchor-positive pairs versus all anchor-positive pairs within a mini-batch, but we found in practice that the all anchor-positive method was more stable and converged slightly faster at the beginning of training.

We also explored the offline generation of triplets in conjunction with the online generation and it may allow the use of smaller batch sizes, but the experiments were inconclusive.

Selecting the hardest negatives can in practice lead to bad local minima early on in training, specifically it can result in a collapsed model (*i.e.* $f(x) = 0$). In order to mitigate this, it helps to select x_i^n such that

$$\|f(x_i^a) - f(x_i^p)\|_2^2 < \|f(x_i^a) - f(x_i^n)\|_2^2 \ . \qquad (4)$$

We call these negative exemplars *semi-hard*, as they are further away from the anchor than the positive exemplar, but still hard because the squared distance is close to the anchor-positive distance. Those negatives lie inside the margin α.

As mentioned before, correct triplet selection is crucial for fast convergence. On the one hand we would like to use small mini-batches as these tend to improve convergence during Stochastic Gradient Descent (SGD) [20]. On the other hand, implementation details make batches of tens to hundreds of exemplars more efficient. The main constraint with regards to the batch size, however, is the way we select hard relevant triplets from within the mini-batches. In most experiments we use a batch size of around 1,800 exemplars.

3.3. Deep Convolutional Networks

In all our experiments we train the CNN using Stochastic Gradient Descent (SGD) with standard backprop [8, 11] and AdaGrad [5]. In most experiments we start with a learning rate of 0.05 which we lower to finalize the model. The models are initialized from random, similar to [16], and trained on a CPU cluster for 1,000 to 2,000 hours. The decrease in the loss (and increase in accuracy) slows down drastically after 500h of training, but additional training can still significantly improve performance. The margin α is set to 0.2.

We used two types of architectures and explore their trade-offs in more detail in the experimental section. Their practical differences lie in the difference of parameters and FLOPS. The best model may be different depending on the application. *E.g.* a model running in a datacenter can have many parameters and require a large number of FLOPS, whereas a model running on a mobile phone needs to have few parameters, so that it can fit into memory. All our models use rectified linear units as the non-linear activation function.

layer	size-in	size-out	kernel	param	FLPS
conv1	220×220×3	110×110×64	7×7×3, 2	9K	115M
pool1	110×110×64	55×55×64	3×3×64, 2	0	
rnorm1	55×55×64	55×55×64		0	
conv2a	55×55×64	55×55×64	1×1×64, 1	4K	13M
conv2	55×55×64	55×55×192	3×3×64, 1	111K	335M
rnorm2	55×55×192	55×55×192		0	
pool2	55×55×192	28×28×192	3×3×192, 2	0	
conv3a	28×28×192	28×28×192	1×1×192, 1	37K	29M
conv3	28×28×192	28×28×384	3×3×192, 1	664K	521M
pool3	28×28×384	14×14×384	3×3×384, 2	0	
conv4a	14×14×384	14×14×384	1×1×384, 1	148K	29M
conv4	14×14×384	14×14×256	3×3×384, 1	885K	173M
conv5a	14×14×256	14×14×256	1×1×256, 1	66K	13M
conv5	14×14×256	14×14×256	3×3×256, 1	590K	116M
conv6a	14×14×256	14×14×256	1×1×256, 1	66K	13M
conv6	14×14×256	14×14×256	3×3×256, 1	590K	116M
pool4	14×14×256	7×7×256	3×3×256, 2	0	
concat	7×7×256	7×7×256		0	
fc1	7×7×256	1×32×128	maxout p=2	103M	103M
fc2	1×32×128	1×32×128	maxout p=2	34M	34M
fc7128	1×32×128	1×1×128		524K	0.5M
L2	1×1×128	1×1×128		0	
total				140M	1.6B

Table 1. **NN1.** This table show the structure of our Zeiler&Fergus [22] based model with 1×1 convolutions inspired by [9]. The input and output sizes are described in $rows \times cols \times \#filters$. The kernel is specified as $rows \times cols, stride$ and the maxout [6] pooling size as $p = 2$.

The first category, shown in Table 1, adds $1\times1\times d$ convolutional layers, as suggested in [9], between the standard convolutional layers of the Zeiler&Fergus [22] architecture and results in a model 22 layers deep. It has a total of 140 million parameters and requires around 1.6 billion FLOPS per image.

The second category we use is based on GoogLeNet style Inception models [16]. These models have $20\times$ fewer parameters (around 6.6M-7.5M) and up to $5\times$ fewer FLOPS (between 500M-1.6B). Some of these models are dramatically reduced in size (both depth and number of filters), so that they can be run on a mobile phone. One, NNS1, has 26M parameters and only requires 220M FLOPS per image. The other, NNS2, has 4.3M parameters and 20M FLOPS. Table 2 describes NN2 our largest network in detail. NN3 is identical in architecture but has a reduced input size of 160x160. NN4 has an input size of only 96x96, thereby drastically reducing the CPU requirements (285M FLOPS vs 1.6B for NN2). In addition to the reduced input size it does not use 5x5 convolutions in the higher layers as the receptive field is already too small by then. Generally we found that the 5x5 convolutions can be removed throughout

with only a minor drop in accuracy. Figure 4 compares all our models.

4. Datasets and Evaluation

We evaluate our method on four datasets and with the exception of Labelled Faces in the Wild and YouTube Faces we evaluate our method on the face verification task. *I.e.* given a pair of two face images a squared L_2 distance threshold $D(x_i, x_j)$ is used to determine the classification of *same* and *different*. All faces pairs (i, j) of the same identity are denoted with $\mathcal{P}_{\text{same}}$, whereas all pairs of different identities are denoted with $\mathcal{P}_{\text{diff}}$.

We define the set of all *true accepts* as

$$\text{TA}(d) = \{(i, j) \in \mathcal{P}_{\text{same}}, \text{with } D(x_i, x_j) \leq d\} \ . \quad (5)$$

These are the face pairs (i, j) that were correctly classified as *same* at threshold d. Similarly

$$\text{FA}(d) = \{(i, j) \in \mathcal{P}_{\text{diff}}, \text{with } D(x_i, x_j) \leq d\} \quad (6)$$

is the set of all pairs that was incorrectly classified as *same* (*false accept*).

The validation rate $\text{VAL}(d)$ and the false accept rate $\text{FAR}(d)$ for a given face distance d are then defined as

$$\text{VAL}(d) = \frac{|\text{TA}(d)|}{|\mathcal{P}_{\text{same}}|} \ , \quad \text{FAR}(d) = \frac{|\text{FA}(d)|}{|\mathcal{P}_{\text{diff}}|} \ . \quad (7)$$

4.1. Hold-out Test Set

We keep a hold out set of around one million images, that has the same distribution as our training set, but disjoint identities. For evaluation we split it into five disjoint sets of 200k images each. The FAR and VAL rate are then computed on 100k $\times$ 100k image pairs. Standard error is reported across the five splits.

4.2. Personal Photos

This is a test set with similar distribution to our training set, but has been manually verified to have very clean labels. It consists of three personal photo collections with a total of around 12k images. We compute the FAR and VAL rate across all 12k squared pairs of images.

4.3. Academic Datasets

Labeled Faces in the Wild (LFW) is the de-facto academic test set for face verification [7]. We follow the standard protocol for *unrestricted, labeled outside data* and report the mean classification accuracy as well as the standard error of the mean.

Youtube Faces DB [21] is a new dataset that has gained popularity in the face recognition community [17, 15]. The setup is similar to LFW, but instead of verifying pairs of images, pairs of videos are used.

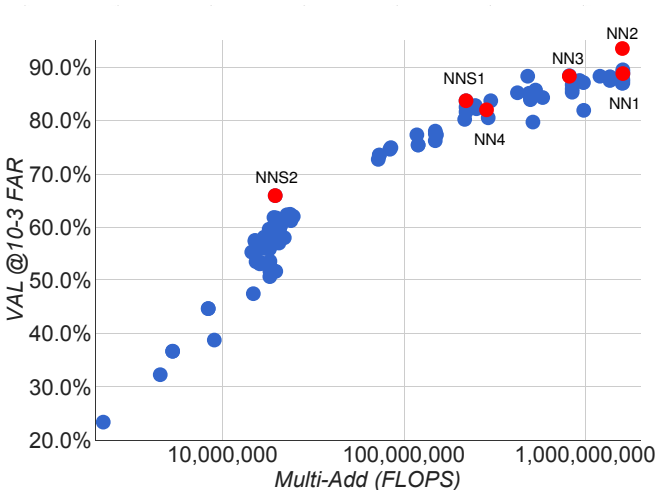


Figure 4. **FLOPS *vs*. Accuracy trade-off.** Shown is the trade-off between FLOPS and accuracy for a wide range of different model sizes and architectures. Highlighted are the four models that we focus on in our experiments.

5. Experiments

If not mentioned otherwise we use between 100M-200M training face thumbnails consisting of about 8M different identities. A face detector is run on each image and a tight bounding box around each face is generated. These face thumbnails are resized to the input size of the respective network. Input sizes range from 96x96 pixels to 224x224 pixels in our experiments.

5.1. Computation Accuracy Trade-off

Before diving into the details of more specific experiments we will discuss the trade-off of accuracy versus number of FLOPS that a particular model requires. Figure 4 shows the FLOPS on the x-axis and the accuracy at 0.001 false accept rate (FAR) on our user labelled test-data set from section 4.2. It is interesting to see the strong correlation between the computation a model requires and the accuracy it achieves. The figure highlights the five models (NN1, NN2, NN3, NNS1, NNS2) that we discuss in more detail in our experiments.

We also looked into the accuracy trade-off with regards to the number of model parameters. However, the picture is not as clear in that case. For example, the Inception based model NN2 achieves a comparable performance to NN1, but only has a 20th of the parameters. The number of FLOPS is comparable, though. Obviously at some point the performance is expected to decrease, if the number of parameters is reduced further. Other model architectures may allow further reductions without loss of accuracy, just like Inception [16] did in this case.

type	output size	depth	#1×1	#3×3 reduce	#3×3	#5×5 reduce	#5×5	pool proj (p)	params	FLOPS
conv1 (7×7×3, 2)	112×112×64	1							9K	119M
max pool + norm	56×56×64	0						m 3×3, 2		
inception (2)	56×56×192	2		64	192				115K	360M
norm + max pool	28×28×192	0						m 3×3, 2		
inception (3a)	28×28×256	2	64	96	128	16	32	m, 32p	164K	128M
inception (3b)	28×28×320	2	64	96	128	32	64	L_2, 64p	228K	179M
inception (3c)	14×14×640	2	0	128	256,2	32	64,2	m 3×3,2	398K	108M
inception (4a)	14×14×640	2	256	96	192	32	64	L_2, 128p	545K	107M
inception (4b)	14×14×640	2	224	112	224	32	64	L_2, 128p	595K	117M
inception (4c)	14×14×640	2	192	128	256	32	64	L_2, 128p	654K	128M
inception (4d)	14×14×640	2	160	144	288	32	64	L_2, 128p	722K	142M
inception (4e)	7×7×1024	2	0	160	256,2	64	128,2	m 3×3,2	717K	56M
inception (5a)	7×7×1024	2	384	192	384	48	128	L_2, 128p	1.6M	78M
inception (5b)	7×7×1024	2	384	192	384	48	128	m, 128p	1.6M	78M
avg pool	1×1×1024	0								
fully conn	1×1×128	1							131K	0.1M
L2 normalization	1×1×128	0								
total									7.5M	1.6B

Table 2. **NN2.** Details of the NN2 Inception incarnation. This model is almost identical to the one described in [16]. The two major differences are the use of L_2 pooling instead of max pooling (m), where specified. *I.e.* instead of taking the spatial max the L_2 norm is computed. The pooling is always 3×3 (aside from the final average pooling) and in parallel to the convolutional modules inside each Inception module. If there is a dimensionality reduction after the pooling it is denoted with p. 1×1, 3×3, and 5×5 pooling are then concatenated to get the final output.

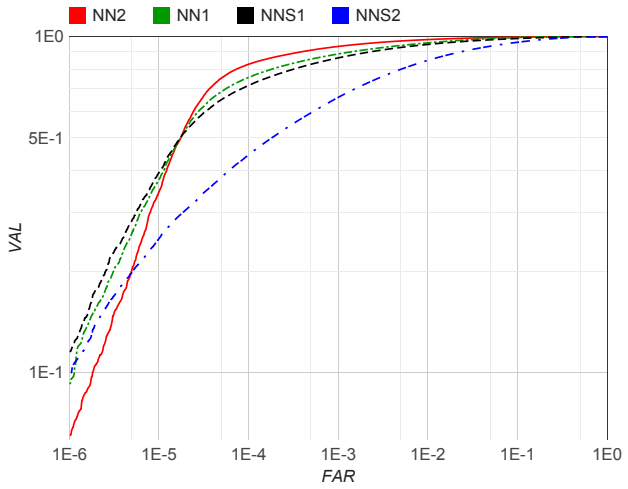


Figure 5. **Network Architectures.** This plot shows the complete ROC for the four different models on our personal photos test set from section 4.2. The sharp drop at 10E-4 FAR can be explained by noise in the groundtruth labels. The models in order of performance are: **NN2:** 224×224 input Inception based model; **NN1:** Zeiler&Fergus based network with 1×1 convolutions; **NNS1:** small Inception style model with only 220M FLOPS; **NNS2:** tiny Inception model with only 20M FLOPS.

architecture	VAL
NN1 (Zeiler&Fergus 220×220)	87.9% ± 1.9
NN2 (Inception 224×224)	89.4% ± 1.6
NN3 (Inception 160×160)	88.3% ± 1.7
NN4 (Inception 96×96)	82.0% ± 2.3
NNS1 (mini Inception 165×165)	82.4% ± 2.4
NNS2 (tiny Inception 140×116)	51.9% ± 2.9

Table 3. **Network Architectures.** This table compares the performance of our model architectures on the hold out test set (see section 4.1). Reported is the mean validation rate VAL at 10E-3 false accept rate. Also shown is the standard error of the mean across the five test splits.

5.2. Effect of CNN Model

We now discuss the performance of our four selected models in more detail. On the one hand we have our traditional Zeiler&Fergus based architecture with 1×1 convolutions [22, 9] (see Table 1). On the other hand we have Inception [16] based models that dramatically reduce the model size. Overall, in the final performance the top models of both architectures perform comparably. However, some of our Inception based models, such as NN3, still achieve good performance while significantly reducing both the FLOPS and the model size.

The detailed evaluation on our personal photos test set is

jpeg q	val-rate
10	67.3%
20	81.4%
30	83.9%
50	85.5%
70	86.1%
90	86.5%

#pixels	val-rate
1,600	37.8%
6,400	79.5%
14,400	84.5%
25,600	85.7%
65,536	86.4%

Table 4. **Image Quality.** The table on the left shows the effect on the validation rate at 10E-3 precision with varying JPEG quality. The one on the right shows how the image size in pixels effects the validation rate at 10E-3 precision. This experiment was done with NN1 on the first split of our test hold-out dataset.

#dims	VAL
64	$86.8\% \pm 1.7$
128	$87.9\% \pm 1.9$
256	$87.7\% \pm 1.9$
512	$85.6\% \pm 2.0$

Table 5. **Embedding Dimensionality.** This Table compares the effect of the embedding dimensionality of our model NN1 on our hold-out set from section 4.1. In addition to the VAL at 10E-3 we also show the standard error of the mean computed across five splits.

shown in Figure 5. While the largest model achieves a dramatic improvement in accuracy compared to the tiny NNS2, the latter can be run 30ms / image on a mobile phone and is still accurate enough to be used in face clustering. The sharp drop in the ROC for FAR $< 10^{-4}$ indicates noisy labels in the test data groundtruth. At extremely low false accept rates a single mislabeled image can have a significant impact on the curve.

5.3. Sensitivity to Image Quality

Table 4 shows the robustness of our model across a wide range of image sizes. The network is surprisingly robust with respect to JPEG compression and performs very well down to a JPEG quality of 20. The performance drop is very small for face thumbnails down to a size of 120x120 pixels and even at 80x80 pixels it shows acceptable performance. This is notable, because the network was trained on 220x220 input images. Training with lower resolution faces could improve this range further.

5.4. Embedding Dimensionality

We explored various embedding dimensionalities and selected 128 for all experiments other than the comparison reported in Table 5. One would expect the larger embeddings to perform at least as good as the smaller ones, however, it is possible that they require more training to achieve the same accuracy. That said, the differences in the performance reported in Table 5 are statistically insignificant.

#training images	VAL
2,600,000	76.3%
26,000,000	85.1%
52,000,000	85.1%
260,000,000	86.2%

Table 6. **Training Data Size.** This table compares the performance after 700h of training for a smaller model with 96x96 pixel inputs. The model architecture is similar to NN2, but without the 5x5 convolutions in the Inception modules.

It should be noted, that during training a 128 dimensional float vector is used, but it can be quantized to 128-bytes without loss of accuracy. Thus each face is compactly represented by a 128 dimensional byte vector, which is ideal for large scale clustering and recognition. Smaller embeddings are possible at a minor loss of accuracy and could be employed on mobile devices.

5.5. Amount of Training Data

Table 6 shows the impact of large amounts of training data. Due to time constraints this evaluation was run on a smaller model; the effect may be even larger on larger models. It is clear that using tens of millions of exemplars results in a clear boost of accuracy on our personal photo test set from section 4.2. Compared to only millions of images the relative reduction in error is 60%. Using another order of magnitude more images (hundreds of millions) still gives a small boost, but the improvement tapers off.

5.6. Performance on LFW

We evaluate our model on LFW using the standard protocol for *unrestricted, labeled outside data*. Nine training splits are used to select the L_2-distance threshold. Classification (*same* or *different*) is then performed on the tenth test split. The selected optimal threshold is 1.242 for all test splits except split eighth (1.256).

Our model is evaluated in two modes:

1. Fixed center crop of the LFW provided thumbnail.
2. A proprietary face detector (similar to Picasa [3]) is run on the provided LFW thumbnails. If it fails to align the face (this happens for two images), the LFW alignment is used.

Figure 6 gives an overview of *all* failure cases. It shows false accepts on the top as well as false rejects at the bottom. We achieve a classification accuracy of **98.87%** ± 0.15 when using the fixed center crop described in (1) and the record breaking **99.63%** ± 0.09 standard error of the mean when using the extra face alignment (2). This reduces the error reported for DeepFace in [17] by more than a factor

Figure 6. **LFW errors.** This shows all pairs of images that were incorrectly classified on LFW. Only eight of the 13 false rejects shown here are actual errors the other five are mislabeled in LFW.

of 7 and the previous state-of-the-art reported for DeepId2+ in [15] by 30%. This is the performance of model NN1, but even the much smaller NN3 achieves performance that is not statistically significantly different.

5.7. Performance on Youtube Faces DB

We use the average similarity of all pairs of the first one hundred frames that our face detector detects in each video. This gives us a classification accuracy of **95.12%**$\pm$0.39. Using the first one thousand frames results in 95.18%. Compared to [17] 91.4% who also evaluate one hundred frames per video we reduce the error rate by almost half. DeepId2+ [15] achieved 93.2% and our method reduces this error by 30%, comparable to our improvement on LFW.

5.8. Face Clustering

Our compact embedding lends itself to be used in order to cluster a users personal photos into groups of people with the same identity. The constraints in assignment imposed by clustering faces, compared to the pure verification task, lead to truly amazing results. Figure 7 shows one cluster in a users personal photo collection, generated using agglomerative clustering. It is a clear showcase of the incredible invariance to occlusion, lighting, pose and even age.

Figure 7. **Face Clustering.** Shown is an exemplar cluster for one user. All these images in the users personal photo collection were clustered together.

6. Summary

We provide a method to directly learn an embedding into an Euclidean space for face verification. This sets it apart from other methods [15, 17] who use the CNN bottleneck layer, or require additional post-processing such as concate-

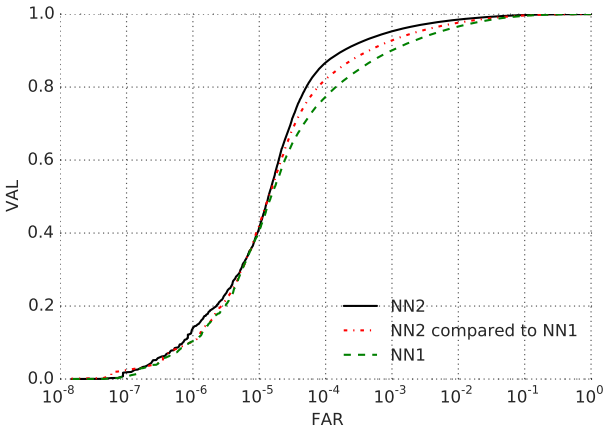


Figure 8. **Harmonic Embedding Compatibility.** These ROCs show the compatibility of the *harmonic* embeddings of NN2 to the embeddings of NN1. NN2 is an improved model that performs much better than NN1. When comparing embeddings generated by NN1 to the *harmonic* ones generated by NN2 we can see the compatibility between the two. In fact, the mixed mode performance is still better than NN1 by itself.

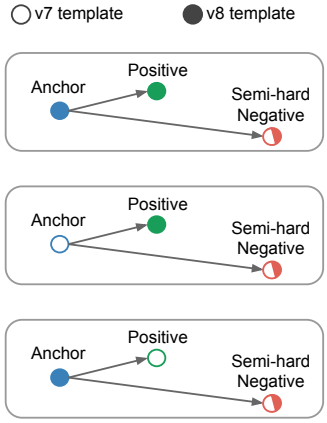


Figure 9. **Learning the Harmonic Embedding.** In order to learn a *harmonic* embedding, we generate triplets that mix the v1 embeddings with the v2 embeddings that are being trained. The semi-hard negatives are selected from the whole set of both v1 and v2 embeddings.

nation of multiple models and PCA, as well as SVM classification. Our end-to-end training both simplifies the setup and shows that directly optimizing a loss relevant to the task at hand improves performance.

Another strength of our model is that it only requires minimal alignment (tight crop around the face area). [17], for example, performs a complex 3D alignment. We also experimented with a similarity transform alignment and notice that this can actually improve performance slightly. It is not clear if it is worth the extra complexity.

Future work will focus on better understanding of the error cases, further improving the model, and also reducing model size and reducing CPU requirements. We will also look into ways of improving the currently extremely long training times, *e.g.* variations of our curriculum learning with smaller batch sizes and offline as well as online positive and negative mining.

7. Appendix: Harmonic Embedding

In this section we introduce the concept of *harmonic* embeddings. By this we denote a set of embeddings that are generated by different models v1 and v2 but are compatible in the sense that they can be compared to each other.

This compatibility greatly simplifies upgrade paths. *E.g.* in an scenario where embedding v1 was computed across a large set of images and a new embedding model v2 is being rolled out, this compatibility ensures a smooth transition without the need to worry about version incompatibilities. Figure 8 shows results on our 3G dataset. It can be seen that the improved model NN2 significantly outperforms NN1, while the comparison of NN2 embeddings to NN1 embeddings performs at an intermediate level.

7.1. Harmonic Triplet Loss

In order to learn the *harmonic* embedding we mix embeddings of v1 together with the embeddings v2, that are being learned. This is done inside the triplet loss and results in additionally generated triplets that encourage the compatibility between the different embedding versions. Figure 9 visualizes the different combinations of triplets that contribute to the triplet loss.

We initialized the v2 embedding from an independently trained NN2 and retrained the last layer (embedding layer) from random initialization with the compatibility encouraging triplet loss. First only the last layer is retrained, then we continue training the whole v2 network with the harmonic loss.

Figure 10 shows a possible interpretation of how this compatibility may work in practice. The vast majority of v2 embeddings may be embedded near the corresponding v1 embedding, however, incorrectly placed v1 embeddings can be perturbed slightly such that their new location in embedding space improves verification accuracy.

7.2. Summary

These are very interesting findings and it is somewhat surprising that it works so well. Future work can explore how far this idea can be extended. Presumably there is a limit as to how much the v2 embedding can improve over v1, while still being compatible. Additionally it would be interesting to train small networks that can run on a mobile phone and are compatible to a larger server side model.

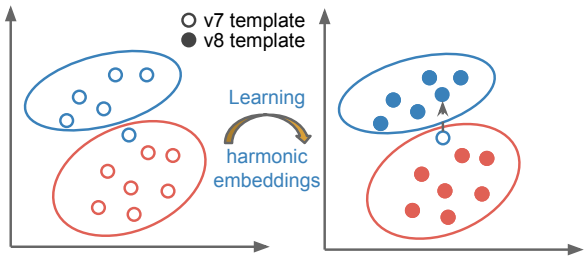


Figure 10. **Harmonic Embedding Space.** This visualisation sketches a possible interpretation of how *harmonic* embeddings are able to improve verification accuracy while maintaining compatibility to less accurate embeddings. In this scenario there is one misclassified face, whose embedding is perturbed to the "correct" location in v2.

Acknowledgments

We would like to thank Johannes Steffens for his discussions and great insights on face recognition and Christian Szegedy for providing new network architectures like [16] and discussing network design choices. Also we are indebted to the DistBelief [4] team for their support especially to Rajat Monga for help in setting up efficient training schemes.

Also our work would not have been possible without the support of Chuck Rosenberg, Hartwig Adam, and Simon Han.

References

[1] Y. Bengio, J. Louradour, R. Collobert, and J. Weston. Curriculum learning. In *Proc. of ICML*, New York, NY, USA, 2009. 2

[2] D. Chen, X. Cao, L. Wang, F. Wen, and J. Sun. Bayesian face revisited: A joint formulation. In *Proc. ECCV*, 2012. 2

[3] D. Chen, S. Ren, Y. Wei, X. Cao, and J. Sun. Joint cascade face detection and alignment. In *Proc. ECCV*, 2014. 7

[4] J. Dean, G. Corrado, R. Monga, K. Chen, M. Devin, M. Mao, M. Ranzato, A. Senior, P. Tucker, K. Yang, Q. V. Le, and A. Y. Ng. Large scale distributed deep networks. In P. Bartlett, F. Pereira, C. Burges, L. Bottou, and K. Weinberger, editors, *NIPS*, pages 1232–1240. 2012. 10

[5] J. Duchi, E. Hazan, and Y. Singer. Adaptive subgradient methods for online learning and stochastic optimization. *J. Mach. Learn. Res.*, 12:2121–2159, July 2011. 4

[6] I. J. Goodfellow, D. Warde-farley, M. Mirza, A. Courville, and Y. Bengio. Maxout networks. In *In ICML*, 2013. 4

[7] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Technical Report 07-49, University of Massachusetts, Amherst, October 2007. 5

[8] Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel. Backpropagation applied to handwritten zip code recognition. *Neural Computation*, 1(4):541–551, Dec. 1989. 2, 4

[9] M. Lin, Q. Chen, and S. Yan. Network in network. *CoRR*, abs/1312.4400, 2013. 2, 4, 6

[10] C. Lu and X. Tang. Surpassing human-level face verification performance on LFW with gaussianface. *CoRR*, abs/1404.3840, 2014. 1

[11] D. E. Rumelhart, G. E. Hinton, and R. J. Williams. Learning representations by back-propagating errors. *Nature*, 1986. 2, 4

[12] M. Schultz and T. Joachims. Learning a distance metric from relative comparisons. In S. Thrun, L. Saul, and B. Schölkopf, editors, *NIPS*, pages 41–48. MIT Press, 2004. 2

[13] T. Sim, S. Baker, and M. Bsat. The CMU pose, illumination, and expression (PIE) database. In *In Proc. FG*, 2002. 2

[14] Y. Sun, X. Wang, and X. Tang. Deep learning face representation by joint identification-verification. *CoRR*, abs/1406.4773, 2014. 1, 2, 3

[15] Y. Sun, X. Wang, and X. Tang. Deeply learned face representations are sparse, selective, and robust. *CoRR*, abs/1412.1265, 2014. 1, 2, 5, 8

[16] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich. Going deeper with convolutions. *CoRR*, abs/1409.4842, 2014. 2, 3, 4, 5, 6, 10

[17] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. Deepface: Closing the gap to human-level performance in face verification. In *IEEE Conf. on CVPR*, 2014. 1, 2, 5, 7, 8, 9

[18] J. Wang, Y. Song, T. Leung, C. Rosenberg, J. Wang, J. Philbin, B. Chen, and Y. Wu. Learning fine-grained image similarity with deep ranking. *CoRR*, abs/1404.4661, 2014. 2

[19] K. Q. Weinberger, J. Blitzer, and L. K. Saul. Distance metric learning for large margin nearest neighbor classification. In *NIPS*. MIT Press, 2006. 2, 3

[20] D. R. Wilson and T. R. Martinez. The general inefficiency of batch training for gradient descent learning. *Neural Networks*, 16(10):1429–1451, 2003. 4

[21] L. Wolf, T. Hassner, and I. Maoz. Face recognition in unconstrained videos with matched background similarity. In *IEEE Conf. on CVPR*, 2011. 5

[22] M. D. Zeiler and R. Fergus. Visualizing and understanding convolutional networks. *CoRR*, abs/1311.2901, 2013. 2, 3, 4, 6

[23] Z. Zhu, P. Luo, X. Wang, and X. Tang. Recover canonical-view faces in the wild with deep neural networks. *CoRR*, abs/1404.3543, 2014. 2

ANNEXE 5

Pièce P-5

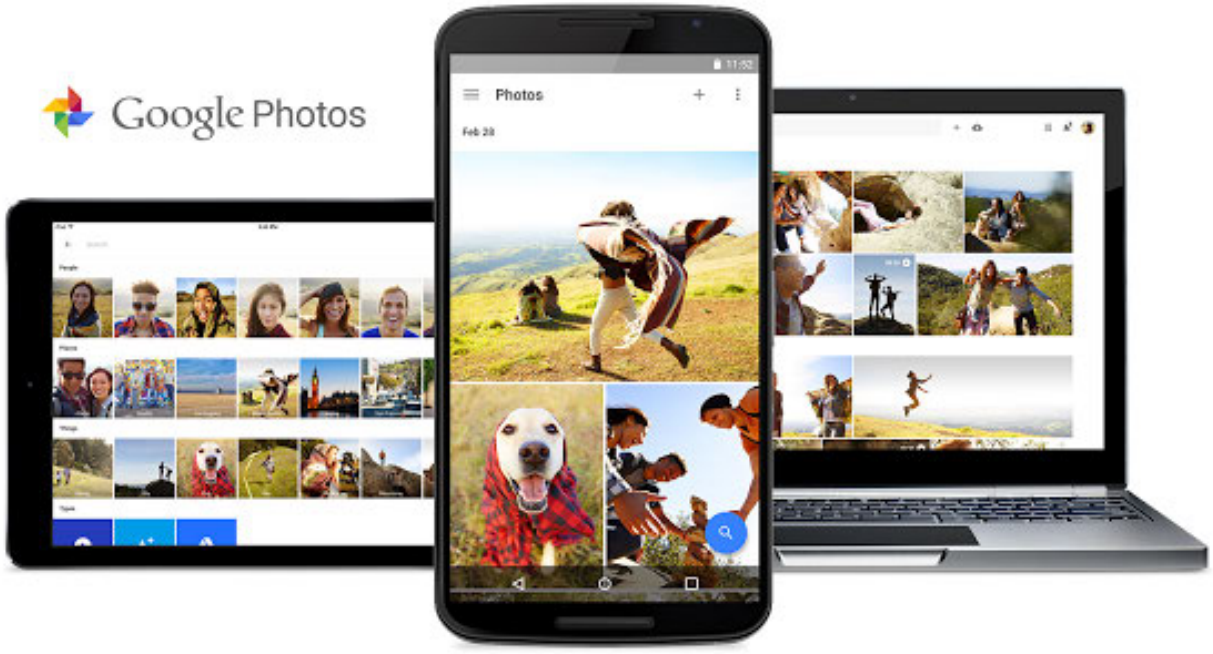
News

PREVIOUS | NEXT

Google Photos update brings facial recognition to Canadian users

By Daniel Bader

OCT 28, 2015 | 4:17 PM EDT | 14 COMMENTS



With version 1.8 on Android, Google Photos will now recognize faces and group them together under the Search button, a feature that was made available to American users after the service was unveiled at Google I/O this past May. With this version, facial tagging has been expanded to Latin America, Canada, the Caribbean, Australia, and New Zealand. The feature should also roll out to iOS users soon.

The way it works sounds a bit creepy, but Google promises that it is not performing anything nefarious: it is merely matching traits of people uploaded to its servers in order to more easily identify them for tagging and sharing purposes. OK, that sounds more than a little creepy, these are things Google does better than anyone, requiring you to relinquish a bit of your privacy in the process.

Google Photos 1.8 also allows you to hide faces you don't want showing up in the list, a side effect of Google's keen machine learning eye; people from sporting events or other communal get-togethers that you don't know can now be easily hidden, which also removes them from the useful "Rediscover this day" card.

According to *Android Police*, Google is set to launch collaboration features for creating and sharing albums in the near future, but that isn't part of this release.

You can wait for Google Photos 1.8 to hit the Google Play Store, or you can manually update from APKMirror.

Source: Android Police

Featured News

Real Canadian Superstore giving some people a second chance at PS5 pre-order

Tesla Model S and X infotainment upgrade costs $3,510 in Canada

FCC filing suggests iPhone 12 may support reverse wireless charging

FCC filing suggests iPhone 12 may support reverse wireless charging

Related Articles

News SEP 30, 2020 | 3:31 PM EDT

New Google Photos editor makes it easier to tweak images on the go

News JUN 30, 2020 | 10:09 AM EDT

New Google Photos design rolling out to users now

News JUL 9, 2020 | 6:02 PM EDT

Google Photos gets shortcut for sorting pics by recently uploaded

News SEP 21, 2020 | 9:01 PM EDT

Google Photos rolls out refreshed share menu

Comments

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

FlamesFan89 • 5 years ago • edited

How/why is this creepy? Is is creepy that if you upload a bunch of photos of flowers that Google is able to group them into one group called "Flowers"? How are you giving up privacy? You willingly uploaded the photos to Google's servers.

The same technology has existed in Picasa for years now, it's in the Photos app on OS X, and I'm sure in plenty of other offerings from other companies.

It's not creepy, it's image recognition. And it's not a privacy breach, as the user has to willingly agree to upload the photos in the first place.

^ | v • Reply • Share ›

SX86 • 5 years ago

I had to turn on the "Group similar faces" option in settings, but the People section doesn't show yet. I'm guessing Google is currently working its processing magic on my photos before I can see the section..

^ | v • Reply • Share ›

Mayoo • 5 years ago

It was available since a while ..... The update only added the option to hide the faces.

^ | v • Reply • Share ›

Tytan McBride • 5 years ago

Nope...not seeing anything different

^ | v • Reply • Share ›

Naaz Charania • 5 years ago

I think what Google is doing is great. One will be able to hide faces which one does not want to see. Great Google.

^ | v • Reply • Share ›

brararsh • 5 years ago

I have this for long time now. It's not tab, just press search and you will see people group.

1 ^ | v 1 • Reply • Share ›

NotARogersEmployee • 5 years ago

Has anyone tried this yet? I updated just now and I still don't see a 'people' section. Only 'places' and 'things'?

^ | v • Reply • Share ›

FlamesFan89 ➚ NotARogersEmployee • 5 years ago

Go into your settings, and there will be an option for grouping people. Turn it off, then on again, and presto.

^ | v • Reply • Share ›

Jared Bedi ➚ NotARogersEmployee • 5 years ago

Weird, I updated this on my Nexus 7 running 6.0 and nothing... updated my phone on 5.1.1 and it shows there... I can run searches on my tablet for the people I've inputted on my phone, but yet they don't show up under search still. Perhaps some syncing needs to happen first.

^ | v • Reply • Share ›

daveloft ➚ NotARogersEmployee • 5 years ago

Yeah no People tab for me either.

^ | v • Reply • Share ›

selonmoi ➚ NotARogersEmployee • 5 years ago

Did you get the 1.8 update first?

^ | v • Reply • Share ›

NotARogersEmployee ➚ selonmoi • 5 years ago

yah, 1.8.0.106438466. App store says i'm up to date.

^ | v • Reply • Share ›

mxmgodin • 5 years ago

Yay!

^ | v • Reply • Share ›

Newsletter Signup

ENTER EMAIL ADDRESS Submit

ANNEXE 6

C A N A D A

PROVINCE OF QUEBEC
DISTRICT OF MONTRÉAL
LOCALITY OF MONTRÉAL

No: 500-06-001123-211

(Class Action)

SUPERIOR COURT

MICHAEL HOMSY

Applicant

v.

GOOGLE LLC

Respondent

APPLICATION FOR AUTHORIZATION TO ADDUCE RELEVANT EVIDENCE AND TO EXAMINE THE APPLICANT
(574 CCP)

TO THE HONOURABLE JUSTICE DONALD BISSON OF THE SUPERIOR COURT, ACTING AS THE DESIGNATED JUDGE IN THE PRESENT CASE, THE RESPONDENT GOOGLE LLC RESPECTFULLY SUBMITS AS FOLLOWS:

I. INTRODUCTION

1. The Respondent Google LLC ("**Google**") hereby seeks the authorization of this Honourable Court to adduce relevant evidence and to examine the Applicant pursuant to article 574, paragraph 3 of the *Code of Civil Procedure*, RLRQ c C-25.01 ("**CCP**").

2. More specifically, Google seeks authorization to adduce as relevant evidence a Sworn Statement of Yael Marzan, Product Manager Lead of Google Photos, and its Annexes A to C, dated September 3, 2021, a copy of which is filed herewith as **Exhibit G-1**, and to examine the Applicant Michael Homsy on the specific circumstances/allegations outlined below.

3. As further detailed below, the Sworn Statement of Yael Marzan (Exhibit G-1) and the examination of the Applicant are relevant and necessary for the Court's analysis of the authorization criteria pursuant to article 575 CCP, and more particularly in order to correct, clarify and explain certain false, incomplete and ambiguous allegations advanced by the Applicant.

II. THE AUTHORIZATION APPLICATION

4. On or about January 15, 2021, the Applicant Michael Homsy filed an *Originating Application for Authorization to Institute a Class Action and to Obtain the Status of Representative* (the "**Authorization Application**") against Google on behalf of the following proposed class (the "**Class**" or the "**Class Members**"):

> **"User class**: All individuals residing in the Province of Quebec, except for the Excluded Persons*, who used Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos since October 28th, 2015 (the "**Class Period**");
>
> **"Non-User Class**: All individuals residing in the Province of Quebec, except for the Excluded Persons, who did not use Google Photos and who had their facial biometric identifiers extracted, collected, captured, received, or otherwise obtained by Google from photos uploaded to Google Photos during the Class Period;
>
> "**Excluded Persons**" means Google and its parent corporations, subsidiaries, affiliates, predecessors, successors and assigns; and their current or former officers, directors, and legal representatives;"

5. The Authorization Application alleges that Google extracted, collected, stored, and used the "facial biometric identifiers" of the Applicant and the Class Members without providing any or adequate notice, without obtaining informed consent and without publishing biometric data retention policies (paras. 2 and 4 of the Authorization Application).

6. More specifically, the Authorization Application alleges that whenever a photo is uploaded to Google Photos, facial biometric identifiers are extracted from any detected face image, without consideration for whether the face belonged to a Google Photo user or non-user (paras. 30 and 31 of the Authorization Application).

7. It is alleged that Google used the Class Members' facial biometric data "for its own competitive advantage in the marketplaces for photo-sharing and other services integrated with Google Photos, which services the Respondent has monetized, or may monetize, through data mining and targeted advertising" (para. 33 of the Authorization Application).

8. The Authorization Application further alleges that the facial biometric identifiers extracted and collected by Google through Google Photos are stored and remain accessible to Google, its personnel, and any third party that Google permits to access such data (para. 32 of the Authorization Application).

9. As a result thereof, the Authorization Application claims that Google (paras. 6-8 of the Authorization Application):

a) Violated Class Members' rights to inviolability and privacy pursuant to the *Charter of Human Rights and Freedoms*, CQLR c C-12;

b) Failed to meet its obligations under the *Civil Code of Quebec*, CQLR c CCQ-1991 and the *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1; and

c) Made misleading representations to the users of Google Photos regarding its privacy practices and policies by omitting or being ambiguous about the fact that it collected and retained sensitive personal information in the form of facial biometric data, the whole in violation of the *Consumer Protection Act,* CQLR.

10. With regard to his particular situation, which the Court must analyze to determine if the proposed class action should be authorized, the Applicant alleges that:

a) On or about the month of March 2020, he purchased an Android Phone and he began using Google Photos after accepting Google's Terms of Use and Privacy Policy (paras. 48-49 of the Authorization Application);

b) He took photos of himself and others using his Android phone and uploaded an estimated 5,500 photos to the platform (paras. 50-51 of the Authorization Application);

c) He did not know that Google was extracting, collecting, storing and using facial biometric identifiers from his photos (para. 52 of the Authorization Application);

d) He was made aware of Google's storage and use of his facial biometric data in January 2021, after which he transferred his photos to Dropbox (paras. 53 and 56 of the Authorization Application);

e) Had he been made aware that Google was storing and using his facial biometric data, he would not have used Google Photos (para. 55 of the Authorization Application);

f) As a result of Google's violation of his right to privacy and inviolability, he suffered damages, including inconveniences, anxiety and pecuniary damages (para. 58 of the Authorization Application);

g) He has also been overcome with feelings of powerlessness, betrayal, fear, stress, and anxiety (para. 59 of the Authorization Application).

III. THE RELEVANCE OF THE SWORN STATEMENT OF YAEL MARZAN

11. Google seeks this Honourable Court's permission to file the Sworn Statement of Yael Marzan, Product Manager Lead of Google Photos dated September 3, 2021 (Exhibit G-1), and the annexes in support thereof, in order to complete and correct certain allegations and evidence advanced in the Authorization Application.

12. Indeed, as will be further detailed below, the Authorization Application makes several vague, ambiguous and/or erroneous allegations with respect to the Google Photos service, its functioning and features, the consent and knowledge of the Applicant Mr. Homsy and of users in respect of the service, the use of the data associated with photos uploaded to Google Photos, third-party access to the data associated with photos uploaded to Google Photos and targeted advertising by Google.

13. The Sworn Statement of Yael Marzan and its supporting annexes A to C (Exhibit G-1) serve to correct these erroneous allegations and to provide all of the relevant and necessary information regarding the Google Photos service, its functioning and features and the optional face grouping feature available for users of Google Photos, in order to provide the Court with a true and complete factual matrix relating to the allegations of the Authorization Application.

14. More specifically, the Sworn Statement of Yael Marzan and its annexes A to C (Exhibit G-1) serves to:

    a) Complete and clarify the vague and ambiguous allegation of the Authorization Application that Google Photos is pre-installed on all Android Phones and automatically uploads photos taken by the user (para. 26 of the Authorization Application), by explaining that automatic uploading of photos is done at the choice of the user;

    b) Complete and clarify the vague and ambiguous allegations of the Authorization Application regarding the Google Photos service (see for example paras. 2, 22 and following of the Authorization Application) by explaining that:

        i. the Google Photos face grouping feature is optional and can be disabled by the user at any time; and

        ii. Google has both consumer accounts and enterprise accounts that operate differently with respect to Google Photos;

    c) Correct and complete the Authorization Application's erroneous allegations that Google was allegedly "extracting, collecting, storing, and using facial biometric identifiers" without the Applicant's and users' knowledge (see for example paras. 2 and 52 of the Authorization Application), by explaining the Google Photos service and features (including namely face grouping which is erroneously described and defined as "biometrics" in the Authorization

Application), and the messages and links shown and/or offered to users and/or non-users regarding the Google Photos service.

d) Complete, clarify and correct the Authorization Application's vague, ambiguous and/or erroneous allegations regarding Google's alleged collection, storage and use of the data associated with photos uploaded to Google Photos (see for example paras. 2, 33, 43, 52-56, 61, 64, 68, 74 and 78 of the Authorization Application), by:

   i. Explaining how Google Photos functions in terms of photo organizing;

   ii. Clarifying that face templates and face groups are private to each user's account;

   iii. Clarifying that "Facenet" (Google's algorithm which processes images of faces) does not attempt to determine a person's identity from a photo; and

   iv. Explaining how the data associated with a photo is stored and deleted;

e) Correct the Authorization Application's erroneous allegations that "facial biometric identifiers" are collected by Google and accessible to third-party developers (see for example para. 32 of the Authorization Application), by confirming that third-party partners who use the Google Photos API (software made available by Google to assist partners to integrate their products with Google Photos) are required to comply with Google's policies and cannot access any user data without the user's permission;

f) Correct the Authorization Application's erroneous allegations that "facial biometric data" is collected by Google and used for its own competitive advantage and for targeted advertising (see for example paras. 33 and 75 of the Authorization Application), by confirming that Google Photos is not used to target advertising and that no third party advertising is displayed on Google Photos whosoever.

15. The Sworn Statement of Yael Marzan and the supporting annexes A to C (Exhibit G-1) thus serve to complete and correct the otherwise vague, ambiguous and/or erroneous allegations of the Authorization Application regarding the Google Photos service generally, including specifically its functioning, features and its use by Google. It provides the Court with the complete factual matrix regarding the allegations advanced by the Applicant in this regard and will assist this Honourable Court in its analysis of the authorization criteria, and specifically in its determination of whether the Applicant has established an arguable case pursuant to article 575 (2) CCP.

IV. THE RELEVANCE AND SCOPE OF THE EXAMINATION OF THE APPLICANT

16. As explained, the Authorization Application offers only general, vague and unsubstantiated assertions with regard to the Applicant's individual cause of action, which must be analyzed to determine whether there is an arguable case against Google (article 575 (2) of the CCP) and the Applicant's ability to properly represent the members of the proposed Class (article 575(4) CCP).

17. In this context, the examination of the Applicant before the hearing of the Authorization Application is both useful and necessary to provide this Honourable Court with the complete and true facts relating to:

    a) The elements giving rise to the Applicant's own personal cause of action as against Google, including the circumstances surrounding:

        i. Any alleged representations the Applicant would have seen and/or relied upon regarding Google Photos' services (see for example paras. 43-44 and 49 of the Authorization Application);

        ii. The Applicant's acceptance of the Terms of Use and Privacy Policy (see paras. 38, 39 and 49 of the Authorization Application);

        iii. The Applicant's actual use of Google Photos (paras. 47-48, 50-51 of the Authorization Application);

        iv. The Applicant's alleged damages, which are only vaguely described as inconveniences, anxiety and pecuniary damages (paras. 58-59 of the Authorization Application);

        v. The Applicant's discovery of Google's alleged practices in January of 2021 (para. 53 of the Authorization Application)

    b) The Applicant's ability to properly represent the members of the proposed class, including the circumstances surrounding:

        i. The manner in which he was called upon to act as an Applicant;

        ii. The representativeness of his personal cause of action in relation to the proposed class members; and

        iii. His personal capacity to properly represent the proposed class.

18. The Applicant's examination regarding these subjects is limited to what is relevant and useful to this Honourable Court's analysis of the criteria for authorization of the class action pursuant to article 575 CCP, and more particularly with regard to

the appearance of right requirement (article 575 (2) CCP) and the Applicant's ability to properly represent the members of the proposed class (article 575 (4) CCP).

19. The examination, which will not exceed two hours, is proportionate to the nature and to the importance of this proposed class action.

20. The Respondent suggests that this examination be held out of court and before the hearing of the Authorization Application.

21. It is thus in the interest of justice and the parties that the Respondent be authorized to adduce as relevant evidence the Sworn Statement of Yael Marzan and the supporting annexes A to C (Exhibit G-1), and to examine the Applicant on the specific above-listed circumstances/allegations.

22. The present Application is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT TO:

GRANT the present motion;

AUTHORIZE the Respondent Google LLC to file a Sworn Statement of Yael Marzan, Product Manager Lead of Google Photos, and its Annexes A to C, dated September 3, 2021 a copy of which is filed herewith as **Exhibit G-1**;

AUTHORIZE the Respondent Google LLC to examine the Applicant Michael Homsy out of court and before the hearing of the *Originating Application for Authorization to Institute a Class Action and to Obtain the Status of Representative* for a maximum of two hours regarding the following subjects:

i. Any representations that the Applicant would have seen and/or relied upon regarding Google Photos' services;

ii. The Applicant's acceptance of the Terms of Use and Privacy Policy;

iii. The Applicant's actual use of Google Photos;

iv. The Applicant's alleged damages, which are only vaguely described as inconveniences, anxiety and pecuniary damages;

v. The Applicant's discovery of Google's alleged practices in January of 2021.

b) The Applicant's ability to properly represent the members of the proposed class, including the circumstances surrounding:

i. The manner in which he was called upon to act as an Applicant;

ii. The representativeness of his personal cause of action in relation to the proposed class members; and

iii. His personal capacity to properly represent the proposed class.

THE WHOLE with legal costs.

Montréal, this September 3, 2021

Fasken Martineau DuMoulin LLP

Fasken Martineau DuMoulin LLP
Attorneys for GOOGLE LLC

800 Victoria Square, Suite 3500
P.O. Box 242
Montréal, Quebec H4Z 1E9
Fax number: +1 514 397 7600

Mtre Noah Boudreau
Phone number: +1 514 394 4521
Email: nboudreau@fasken.com

Mtre Mirna Kaddis
Phone number: +1 514 397 7484
Email: mkaddis@fasken.com

N° : 500-06-001123-211

PROVINCE OF QUEBEC
DISTRICT OF MONTRÉAL
LOCALITY OF MONTRÉAL

MICHAEL HOMSY

Applicant

v.

GOOGLE LLC

Respondent

16989/311868.00035 BF1339

APPLICATION FOR AUTHORIZATION TO ADDUCE RELEVANT EVIDENCE AND TO EXAMINE THE APPLICANT, NOTICE OF PRESENTATION, LIST OF EXHIBIT AND EXHIBIT G-1

ORIGINAL

Fasken Martineau DuMoulin LLP
800 Victoria Square, Suite 3500
P.O. Box 242
Montréal, Quebec H4Z 1E9

Me Noah Boudreau
nboudreau@fasken.com
Tél. +1 514 394 4521
Fax. +1 514 397 7600

Me Mirna Kaddis
mkaddis@fasken.com
Tél. +1 514 3977484
Fax. +1 514 397 7600

PREUVE DE SIGNIFICATION

ATTORNEY OR PARTY WITHOUT ATTORNEY *(Name, State, Bar number, and address):*	*FOR COURT USE ONLY*
CaLex Légal Inc. **4214 rue Saint-Jacques** **Montreal, Quebec, H4C 1J4** **Canada** TELEPHONE NO.: **514-548-3023** FAX NO. *(Optional)*: E-MAIL ADDRESS *(Optional)*: ATTORNEY FOR *(Name)*: **MICHAEL HOMSY**	
COUR D'APPEL QUEBEC PROVINCE, DISTRICT OF MONTREAL CANADA STREET ADDRESS: **633 Yesler Way** MAILING ADDRESS: **633 Yesler Way** CITY AND ZIP CODE: **Seattle 98104** BRANCH NAME:	
PLAINTIFF/PETITIONER: **MICHAEL HOMSY**	CASE NUMBER:
DEFENDANT/RESPONDENT: **GOOGLE, LLC**	**500-06-001123-311**

PROOF OF SERVICE (CIVIL)	HEARING DATE/TIME:	HEARING DEPT./DIV.:	Ref. No. or File No.: **REF-9820414**

1. At the time of service I was at least 18 years of age and not a party to this action.

BY FAX

2. I served copies of *(specify documents):*
   DECLARATON D'APPEAL

3. a. Party served *(specify name of party as shown on documents served):*
   GOOGLE, LLC

   b. ☐ Person (other than the party in item 3a) served on behalf of an entity or as an authorized agent (and not a person under item 5b whom substituted service was made) *(specify name and relationship to the party named in item 3a):*

4. Address where the party was served:
   C/O CORPORATION SERVICE COMPANY, REGISTERED AGENT, 2710 GATEWAY OAKS DR, STE 150N, SACRAMENTO, CA 95833

5. I served the party *(check proper box)*

   a. ☐ **by personal service.** I personally delivered the documents listed in item 2 to the party or person authorized to receive service of process for the party (1) on *(date):* at *(time):*

   b. ☒ **by substituted service.** On *(date):* **03/29/2022** at *(time):* **8:47 AM** I left the documents listed in item 2 with or in the presence of *(name and title or relationship to person indicated in item 3):*
   Trudy Desbiens, I delivered the documents to Trudy Desbiens who indicated they were the registered agent, co-resident with identity confirmed by subject saying yes when named. The individual accepted service with direct delivery. The individual appeared to be a brown-haired Asian female contact 25-35 years of age, 5'4"-5'6" tall and weighing 140-160 lbs.

   (1) ☒ **(business)** a person at least 18 years of age apparently in charge at the office or usual place of business of the person to be served. I informed him or her of the general nature of the papers.

   (2) ☐ **(home)** a competent member of the household (at least 18 years of age) at the dwelling house or usual place of abode of the party. I informed him or her of the general nature of the papers.

   (3) ☐ **(physical address unknown)** a person at least 18 years of age apparently in charge at the usual mailing address of the person to be served, other than a United States Postal Service post office box. I informed him or her of the general nature of the papers.

   (4) ☒ I thereafter mailed (by first-class, postage prepaid) copies of the documents to the person to be served at the place where the copies were left (Code Civ. Proc., § 415.20). I mailed the documents on *(date):* from *(city):* **or** ☒ a declaration of mailing is attached.

   (5) ☒ I attach a **declaration of diligence** stating actions taken first to attempt personal service.

PLAINTIFF/PETITIONER: MICHAEL HOMSY	CASE NUMBER:
DEFENDANT/RESPONDENT: GOOGLE, LLC	500-06-001123-311

c. ☐ **by mail and acknowledgement of receipt of service.** I mailed the documents listed in item 2 to the party, to the address shown in item 4, by first-class mail, postage prepaid,

(1) on *(date):* (2) from *(city):*

(3) ☐ with two copies of the *Notice and Acknowledgement of Receipt* and a postage-paid return envelope addressed to me. *(Attach completed Notice and Acknowledgement of Receipt.)* (Code Civ. Proc., § 415.30)

(4) ☐ to an address outside California with return receipt requested. (Code Civ. Proc., § 415.40)

d. ☐ **by other means** *(specify means of service and authorizing code section):*

☐ Additional page describing service is attached.

6. **Person who served papers**

a. Name: **Tonya Gutierrez**
b. Address: **1016 galleon way, Sacramento, CA 95838**
c. Telephone number: **916-889-2818**
d. The fee for service was: **$ 95.00**
e. I am:

(1) ☐ not a registered California process server.

(2) ☐ exempt from registration under Business and Professions Code section 22350(b).

(3) ☒ registered California process server:

(i) ☐ owner ☐ employee ☒ independent contractor. For: **ABC Legal Services, LLC**

(ii) ☒ Registration No.: **2018-063** Registration #: **6779**

(iii) ☒ County: **Sacramento CA** County: **Los Angeles**

BY FAX

7. ☒ **I declare** under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

or

8. ☐ **I am a California sheriff or marshal and I certify** that the foregoing is true and correct.

Date: 03/29/2022

Tonya Gutierrez
(NAME OF PERSON WHO SERVED PAPERS/SHERIFF OR MARSHAL)

Tonya Gutierrez
(SIGNATURE)

PROOF OF SERVICE (CIVIL)

REF: **REF-9820414**

Tracking #: **0084925331**

ATTORNEY OR PARTY WITHOUT ATTORNEY *(Name, State, Bar number, and address):*	*FOR COURT USE ONLY*
CaLex Légal Inc. **4214 rue Saint-Jacques** **Montreal, Quebec, H4C 1J4** **Canada** TELEPHONE NO.: **514-548-3023** FAX NO. *(Optional)*: E-MAIL ADDRESS *(Optional)*: ATTORNEY FOR *(Name)*: **MICHAEL HOMSY**	
COUR D'APPEL QUEBEC PROVINCE, DISTRICT OF MONTREAL CANADA STREET ADDRESS: **633 Yesler Way** MAILING ADDRESS: **633 Yesler Way** CITY AND ZIP CODE: **Seattle 98104** BRANCH NAME:	
PLAINTIFF/PETITIONER: **MICHAEL HOMSY**	CASE NUMBER:
DEFENDANT/RESPONDENT: **GOOGLE, LLC**	**500-06-001123-311**

DECLARATION OF REASONABLE DILIGENCE	HEARING DATE/TIME:	HEARING DEPT./DIV.:	Ref. No. or File No.: **REF-9820414**

Party to Serve:
GOOGLE, LLC

Documents:
DECLARATON D'APPEAL

Service Address:
C/O CORPORATION SERVICE COMPANY, REGISTERED AGENT, 2710 GATEWAY OAKS DR, STE 150N, SACRAMENTO, CA 95833

BY FAX

I declare the following attempts were made to effect service by personal delivery:

Person who performed diligence:
Tonya Gutierrez
1016 galleon way, Sacramento, CA 95838
916-889-2818

I am a registered California process server
Registration No.: 2018-063
County: Sacramento CA

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct.
Date: _____

Tonya Gutierrez
(NAME OF PERSON WHO PERFORMED DILIGENCE)

_____
(SIGNATURE)

L'intimé, les intervenants et les mis en cause doivent, dans les 10 jours de la notification, déposer un acte de représentation indiquant le nom et les coordonnées de l'avocat qui les représente ou, dans le cas d'absence de représentation, un acte indiquant ce fait. Cependant, s'il est joint à la déclaration d'appel une demande pour obtenir la permission d'appeler, les intervenants et les mis en cause ne sont tenus de le faire que dans les 10 jours du jugement qui accueille cette demande ou, le cas échéant, de la date à laquelle le juge a pris acte du dépôt de la déclaration. (article 358, al. 2 C.p.c.)

No. C.A. 500-09-029982-220
No. C.S.M. 500-06-001123-211

COUR D'APPEL DU QUÉBEC
DISTRICT DE MONTRÉAL

MICHAEL HOMSY

APPELANT-Demandeur

c.

GOOGLE LLC

INTIMÉE-Défenderesse

DÉCLARATION D'APPEL ET ANNEXES

Partie appelante

Datée du 28 mars 2022

CaLex Légal Inc. | Investigation Counsel PC
4214 rue St-Jacques | 350 Bay St.
Montréal, QC, H4C1J4 | Toronto, ON, M5H2S6
T: +1 514.548.3023 | 416.637.3152
F: +1 514.846.8844 | 416.637.3445
Avocats de l'Appelant
MICHAEL HOMSY
Me Jean-Philippe Caron | Me John Archibald
Me Alessandra Esposito Chartrand | Me Gabriel Bois
Benjamin Tavernier-Labrie, Stagiaire en droit
jpc@calex.legal | aec@calex.legal
gb@calex.legal | btl@calex.legal
jarchibald@investigationcounsel.com
BP3268

Les parties notifient leurs actes de procédure (incluant mémoire ou exposé) à l'appelant et aux seules parties qui ont produit un acte de représentation (ou de non-représentation). (article 25 al. 1 du Règlement de procédure civile) Si une partie est en défaut de produire un acte de représentation (ou de non-représentation), elle ne peut déposer aucun autre acte de procédure au dossier. L'appel procède en son absence. Le greffier n'est tenu de lui notifier aucun avis. Si l'acte est produit en retard, le greffier l'accepte aux conditions qu'il détermine. (article 30 du Règlement de procédure civile)