



Amendment filed pursuant to Rule 6-1(1)(b)(ii)
of the Supreme Court Civil Rules; Original filed on April 6, 2020

NO. VLC-S-S-203879
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

GABRIEL GUESE

PLAINTIFF

AND:

ZOOM MEDIA VIDEO COMMUNICATIONS, INC.

DEFENDANTS

FURTHER AMENDED NOTICE OF CIVIL CLAIM

Brought pursuant to the *Class Proceedings Act*, RSBC 1996, c. 50

This action has been started by the plaintiff for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must:

- (a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must:

- (a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above named registry of this court within the time for response to civil claim described below, and
- (b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

TIME FOR RESPONSE TO CIVIL CLAIM

A response to civil claim must be filed and served on the plaintiff,

- (a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,
- (b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,
- (c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or
- (d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF

Part 1: STATEMENT OF FACTS

The Plaintiff

1. The plaintiff, Gabriel Guese, is an Educational Assistant and has an address for delivery at 1750 – 700 West Georgia Street in Vancouver, British Columbia.

The Defendant

2. The defendant, Zoom ~~Media~~ Video Communications, Inc. (“Zoom”), is a company incorporated pursuant to the laws of the State of Delaware, in the United States of America, with its headquarters at 55 Almaden Boulevard, 6th Floor, San Jose, California.

~~Facts and Averments~~

The Proposed Class

2A. The plaintiff brings this action on his own behalf and on behalf of a national class of all Canadian residents whose personal information or data, including their device and system attributes, were disclosed by Zoom to a third party (collectively the “Class” or “Class Members”) persons in Canada who had a registered Zoom meetings user account or a paid Zoom meetings subscription as of June 30, 2020 and who:

- a. registered, used, opened or downloaded the Zoom meetings application between April 1, 2018 and June 30, 2020; or
- b. paid money to Zoom for a Zoom meetings subscription between April 1, 2018 and June 30, 2020,

but excluding Enterprise and Business Subscribers as of June 30, 2020 and End User Accounts associated with Enterprise and Business Subscribers as of June 30, 2020.

“Enterprise and Business Subscribers” means purchasers of Zoom Meetings licenses for the “Enterprise,” “Business,” or “Business Plus” levels of Zoom’s pricing plans (as opposed to other account types, including “Basic” or “Pro” levels (see [<https://zoom.us/pricing>]), plus any purchaser of 100 or more Zoom Meetings licenses.

“End User Account” means a Zoom Meetings user account that belonged to, was controlled by, or was provisioned by a person paying for a Zoom Meetings subscription.

(collectively, the “Class” or “Class Members”).

Background

3. Zoom produces and provides for use to Canadian individuals, ~~and corporations, and other businesses~~, an online video conferencing platform (referred to as “Zoom Meetings” herein), that enables users to videoconference for business, education, personal, family, and social purposes. The use of Zoom’s videoconferencing technology has become widespread, and increased exponentially with the COVID-19 pandemic.

4. Users of Zoom may use its Zoom Meetings videoconferencing service through Zoom apps or programs on various platforms, including iOS and iPadOS (Apple's mobile operating systems), Android, MacOS (Apple's desktop and laptop operating system), and Windows ~~an App for iOS (Apple’s mobile operating system), an App for Android Devices, an App for MacOS (Apple’s desktop and laptop operating system)~~ (collectively the “Zoom App”).

5. Zoom’s videoconferencing service can also be accessed through a web browser.

6. At all material times, in ~~In~~ the Apple iOS app store, the Zoom App was ~~is~~ called “ZOOM Cloud Meetings”. The marketing description for the Zoom App in the iOS App store stated ~~states~~, in part, ~~as follows~~:

Stay connected wherever you go – start or join a meeting with flawless video, crystal clear audio, instant screen sharing, and cross-platform instant messaging – for free!

Zoom is #1 in customer satisfaction and the best meeting experience on mobile.

Zoom’s Stated Commitment to Privacy

7. At all material times, on ~~On~~ Zoom’s website, www.zoom.us/privacy-and-legal, Zoom stated ~~states~~, “You ~~can~~ trust us to connect you to the people that matter. We value that trust more than anything else. We want you to know what data we collect and how we use it to provide our service.” A link was ~~is~~ provided to Zoom’s privacy policy (~~the~~ “Privacy Policy”).

8. In Zoom’s December 31, 2019 privacy policy (the “Privacy Policy”), which was the policy in effect when Zoom users’ personal information and data was initially disclosed to Facebook, Google, and other third parties without Zoom users’ consent, Zoom purported ~~purports~~ to identify and disclose to its users all the information and data Zoom automatically collected ~~collects~~ from its users when they used its services and how that information and data was protected from unauthorized access, use, or disclosure.

9. Zoom stated ~~states~~ in the Privacy Policy as follows concerning the measures it takes to protect its users’ personal data:

Zoom Privacy Policy

As used in this Privacy Policy, “Personal Data” means any information that can be used to identify or is reasonably linkable to a specific person.

...

Security of your Personal Data

Zoom is committed to protecting the Personal Data you share with us. We utilize a combination of industry-standard security technologies, procedures, and organizational measures to help protect your Personal Data from unauthorized access, use, or disclosure...

10. Despite Zoom’s representations, warranties, and assurances as stated in the Privacy Policy and elsewhere — and in breach of the Privacy Policy — it Zoom included code in the Zoom App that made ~~undisclosed~~ unauthorized disclosures of its users’ personal information and data to Facebook, Google, and ~~potentially~~ other third parties (including third-party developers who develop and deploy apps that integrate with Zoom’s products), and Zoom’s videoconferencing (whether accessed through the Zoom App or through a web browser) did not have end-to-end encryption, contrary to Zoom’s representations that it did.

10A. The representations made by Zoom in the Privacy Policy were false, deceptive, and misleading, and constituted an unfair business practice.

Unauthorized Data Breach

Facebook SDK

11. On March 26, 2020, Joseph Cox posted a report on a web-based news site called Motherboard, operated by Vice Media Group, revealing that the Zoom App contained code that ~~made~~ makes unauthorized disclosure of users’ personal information and data to Facebook—when a Zoom user installed the Zoom App, and each ~~Each~~ time the user opened or closed ~~opens~~ the Zoom App, the

11A. The personal information and data disclosed by Zoom to Facebook and other third parties included, the user’s device model, the time zone and city they are connecting from, the user’s phone/tablet carrier, the OS type and version they are using, their application bundle identifier, their application instance identifier, their application version, their iOS device CPU cores, their iOS device disk space available, their iOS device display dimensions, their iOS language used, and ~~their~~ a unique advertiser identifier — which is automatically created by the user’s device, which can be used to target the user with advertisements.

12. The disclosed personal information and data — either independently or in the aggregate — could be and was used to identify specific Class Members and was reasonably linkable to each specific Class Member. The disclosed information and data were then used by Facebook and other third parties to track Class Members online, target them with advertisements, tailor website content to them, and adjust market pricing upwards for goods being purchased by Class Members online.

13. This personal information and data was disclosed by Zoom to Facebook and other third parties regardless of whether the user had a Facebook account and was disclosed without the Zoom user's consent or knowledge. This disclosure was contrary to and in breach of Zoom's Privacy Policy.

14. Zoom knew, or ought to have known, that the plaintiff's and other Class Members' personal information and data was being collected and disclosed to Facebook and other third parties through Zoom's use of Facebook's software development kit ("SDK"). Facebook's terms of use for its SDK clearly state that, if Facebook's SDK is used by an app developer, Facebook and other third parties will receive, use, and share app users' information and data from the developer's app. Because of this, Facebook requires that a developer using Facebook's SDK represent and warrant that the developer has provided robust notice to the users of its app regarding the collection, sharing, and usage of the customers' information and data. In the March 26, 2020 Motherboard article, it states:

Facebook told Motherboard it requires developers to be transparent with users about the data their apps send to Facebook. Facebook's terms say "If you use our pixels or SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage," and specifically for apps, "that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads."

15. Zoom, in using Facebook's SDK for the purpose of implementing its "Login with Facebook" feature on the Zoom App, represented and warranted to Facebook that it provided the plaintiff and other Class Members with robust and sufficiently prominent notice regarding the collection, sharing, and usage of Class Members' personal information and data to Facebook and other third parties. In breach of the terms of its agreement with Facebook, Zoom did not provide such notice to the plaintiff and other Class Members.

16. Zoom knew, or ought to have known, that the plaintiff's and Class Members' personal information and data were vulnerable to unauthorized data breaches. Zoom failed to use reasonable care in the collection, storage, and retention of the plaintiff's and other Class Members' personal information and data, and Zoom failed to use reasonable care to ensure that this information and

data was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party.

17. Zoom did not contact the plaintiff and other Class Members to disclose the unauthorized data breaches.

18. Neither did Zoom ensure that Facebook, or any other third party, take steps to delete the plaintiff's and other Class Members' private information and data that had been disclosed to them by Zoom without Class Members' consent.

19. On March 27, 2020, Zoom posted an entry on its blog, located on its website, admitting that the Zoom App was sending Zoom users' information and data to Facebook and other third parties (the "Privacy Breach"). Zoom admitted that the unauthorized disclosures began when Zoom contracted with Facebook and implemented a "Login with Facebook" feature using Facebook's SDK.

20. In its March 27, 2020 blog post, Zoom stated:

Zoom takes its users' privacy extremely seriously. We would like to share a change that we have made regarding the use of Facebook's SDK.... Our customers' privacy is incredibly important to us, and therefore we decided to remove the Facebook SDK in our iOS client and have reconfigured the feature so that users will still be able to log in with Facebook via their browser.... We sincerely apologize for the concern this has caused, and remain firmly committed to the protection of our users' privacy. We are reviewing our processes and protocols for implementing these features in the future to ensure this does not happen again.

21. On March 27, 2020, Zoom released an updated version of the Zoom App which purported to no longer disclose its users' personal information and data to Facebook. In its March 27, 2020 blog post, Zoom advised that "[u]sers will need to update to the latest version of our application... in order for these changes to take hold, and we strongly encourage them to do so". The update to the Zoom App therefore required Class Members to take the affirmative step of updating the Zoom App.

22. Zoom did not contact the plaintiff and other Class Members to advise that they needed to update the Zoom App to avoid any further unauthorized disclosure of their personal information

and data to Facebook or other third parties. And Zoom did not take any positive steps to block earlier versions of the Zoom App.

23. Zoom used the “Login with Facebook” feature to add credibility to its videoconferencing services and to attract new Zoom users — which it did. And in doing so, the number of Zooms users and the price of Zoom’s stock increased, as did the value of Zoom generally. Zoom received financial gain and was enriched from implementing the “Login with Facebook” feature, while the plaintiff and other Class Members suffered a corresponding deprivation. There was no juristic reason for Zoom’s enrichment and Class Members’ deprivation.

~~12. The compensation Zoom receives from Facebook, and potentially other third parties, for unauthorized disclosure of personal information is unknown.~~

Firestore Analytics SDK

24. In certain versions of the Zoom App for Android devices, Zoom included the Google Analytics for Firebase SDK (“Firestore SDK”).

25. The Firestore SDK sent device and system information of Android users to Google and, therefore, made unauthorized disclosure of these users’ personal information and data to Google when a Zoom user used the Zoom App.

26. The personal information and data disclosed by Zoom to Google included the user’s device manufacturer and model, the device language settings, the application version they are using, information about app usage, and their unique Android Advertising identifier.

27. The disclosed personal information and data — either independently or in the aggregate — could be and was used to identify specific Class Members and was reasonably linkable to each specific Class Member. The disclosed information and data were then used by Google and other third parties to track Class Members online, target them with advertisements, tailor website content to them, and adjust market pricing upwards for goods being purchased by Class Members online.

28. Zoom knew, or ought to have known, that the plaintiff's and other Class Members' personal information and data was being collected and disclosed to Google through the Firebase SDK.

29. Zoom failed to use reasonable care in the collection, storage, and retention of the plaintiff's and other Class Members' personal information and data, and Zoom failed to use reasonable care to ensure that this information and data was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party.

30. Zoom did not contact the plaintiff and other Class Members to disclose the unauthorized data breaches.

Zoom's Misrepresentations on its use of End-to-End Encryption

31. End-to-end encryption refers to forms of communications where only the communicating users can read or view the communications. Only the communicating users have access to the cryptographic keys that are necessary to encrypt or decrypt the communication, so a third party — including the service providing the communications platform — cannot read or view the communications.

32. End-to-end encryption provides a high standard of security and privacy to the users of internet communication services and has been implemented and offered by Zoom's competitors.

33. Consistent with Zoom's statements about the importance of user privacy, Zoom represented its videoconferencing services as being secured by end-to-end encryption.

34. Zoom's representations about its videoconferencing being encrypted included:

- a. starting as early as July 2017 and continuing through at least April 2020, Zoom asserted that its videoconferencing services provided "industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings";
- b. in its Security Guide, dated June 2019, Zoom made repeated references to end-to-end encryption, including:

i. “The following pre-meeting security capabilities are available to the meeting host”:

- “Enable an end-to-end (E2E) encrypted meeting ...”; and

- “E Chat Encryption: Zoom E2E chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses public and private keys to encrypt the chat session with Advanced Encryption Standard (AES-256). Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped on or tampered with”; and

ii. “The following in-meeting security capabilities are available to the meeting host”:

- “Secure a meeting with E2E encryption ...”; and

c. during teleconferencing meetings, the Zoom App displayed a green lock with an “E” in that stated: “Zoom is using an end to end encrypted connection.”

(collectively, the “E2E Representations”).

35. Through the E2E Representations, Zoom marketed itself as privacy- and security-conscious, and it marketed its videoconferencing services as suitable for those concerned about security and privacy.

36. However, contrary to Zoom’s marketing and the E2E Representations, Zoom acknowledged — in a blog post dated April 1, 2020 — that it had “incorrectly suggest[ed] that Zoom meetings were capable of using end-to-end encryption”.

37. At all material times, Zoom knew — or ought to have known — that the E2E Representations were false. Despite this knowledge, Zoom made the E2E Representations, and it did so with the intent of inducing people to rely on the misrepresentations by using Zoom’s

videoconferencing services. And people did, in fact, rely on the E2E Representations by using Zoom’s videoconferencing services.

38. On or around October 14, 2020, Zoom announced that, starting the following week, “Zoom’s end-to-end encryption (E2EE) offering [would] be available as a technical preview”. This, and Zoom’s subsequent introduction of end-to-end encryption, is contrary to its previous marketing and the E2E Representations, that it had offered end-to-end encryption as far back as July 2017.

The Plaintiff’s Experience with Zoom

13. 39. The plaintiff installed downloaded the Zoom App on March 18, 2020 on two Apple iOS devices prior to March 27, 2020 and used the Zoom App on several occasions both before and after March 27, 2020, including on March 25 and 26, 2020.

40. Contracts existed between Zoom and Class Members, all of which were identical or substantially similar vis-à-vis Zoom and Class Members. When the plaintiff and other Class Members installed and opened the Zoom App or when they otherwise opened Zoom’s videoconferencing services, they agreed – for good and valuable consideration — to allow Zoom to collect and retain their personal information and data. Zoom correspondingly agreed — for good and valuable consideration – to be bound by the Privacy Policy and ensure that the personal privacy of the plaintiff and other Class Members was protected in accordance with the Privacy Policy by utilizing a combination of industry-standard security technologies, procedures and organizational measures — including end-to-end encryption — to protect Class Members’ personal information and data from unauthorized access, use or disclosure. Zoom breached the Privacy Policy and its contractual terms by, among other things, disclosing Class Members’ personal information and data to Facebook, Google, and other third parties. Zoom’s conduct was also contrary to the E2E Representations.

41. The personal information and data provided to Zoom by the plaintiff and other Class Members was confidential and was communicated to Zoom in confidence. The information was misused by Zoom, to the detriment of the plaintiff and other Class Members.

42. Zoom's unauthorized disclosure to Facebook, Google, and other third parties of the plaintiff's and other Class Members' confidential personal information and data was intentional and reckless and, without lawful justification, invaded the private affairs and concerns of the plaintiff and other Class Members. The information and data of the plaintiff and other Class Members were misused by Zoom to the detriment of the plaintiff and other Class Members. The information disclosed — either independently or in the aggregate — was inherently revealing and private, and a reasonable person would regard this invasion as highly offensive causing distress, humiliation, or anguish.

43. Zoom's conduct was in violation of the Privacy Policy, was contrary to the E2E Representations, and substantially, unreasonably, wilfully, and without claim of right violated the privacy of the plaintiff and other Class Members.

44. The plaintiff and other Class Members had the right to personal security and the right to non-disclosure of their confidential information and data, and Zoom intentionally and unlawfully interfered with these rights and freedoms.

14. 45. Had Zoom informed the plaintiff and other Class Members ~~its user~~ that it would use inadequate security measures and disclose their personal information and data to Facebook, Google, and potentially to other third parties without their consent (when the plaintiff and other users installed the Zoom App and every time that the Zoom App was opened or closed by them), and that communications made using Zoom's videoconferencing services were not, in fact, protected by end-to-end encryption, the Plaintiff, and other users, would have chosen not to use Zoom or they and would have used another videoconferencing service that did not disclose — without their authorization — their personal information and data to third parties and that was protected by end-to-end encryption.

46. As a consequence of Zoom's conduct and the unauthorized data breaches, the plaintiff and other Class Members had their privacy deeply invaded and have suffered loss and damage, including but not limited to:

- (a) mental distress;
- (b) humiliation;

- (c) anguish;
- (d) stress;
- (e) anxiety;
- (f) paying more for the goods and services they purchase online than they otherwise would have;
- (g) being subjected to targeted advertisements;
- (h) being subjected to tailored website content to them; and
- (i) out-of-pocket expenses.

15. — ~~Zoom’s statements in its Privacy Policy regarding the protection of its users’ privacy and its purported full disclosure of the manner in which its users’ personal information will be used is false and misleading, and constitutes: a “deceptive act or practice” as defined in section 4 (1) of the British Columbia *Business Practices and Consumer Protection Act*, S.B.C 2004, c.2; an “unfair practice” as defined in section 6 of the Alberta *Consumer Protection Act*, R.S.A. 2000 c. C-26.3; an “unfair practice” as defined in section 6 of the Saskatchewan *Consumer Protection and Business Practices Act*, S.S. 2013, c. C-30.2; an “unfair practice” as defined in section 14 of the Ontario *Consumer Protection Act*, 2002, S.O. 2002, c. C-30, Sched. A; a “false or misleading representation” as defined in section 219 of the Quebec *Consumer Protection Act*, S.Q. c. P-40.1; and an “unfair business practice” as defined in section 7 of the Newfoundland *Consumer Protection and Business Practices Act*, S.N.L., 2009, c. C-31.1.~~

16. — ~~Zoom’s failure to implement adequate security protocols, failure to provide adequate disclosure, and its disclosure of its users’ personal information, breaches Zoom’s assurances to its users and constitutes the tort of intrusion upon seclusion in Canadian jurisdictions where the tort is applicable.~~

17. — ~~Zoom’s failure to implement adequate security protocols, failure to provide adequate disclosure, and its disclosure of its user’s personal information, breaches Zoom’s assurances to its users and constitutes a breach of the British Columbia *Privacy Act*, R.S.B.C. 1996, c.63; the Manitoba *Privacy Act*, CCSM c.P125; the Saskatchewan *Privacy Act*, RSS 1978, c. P-24; and the Newfoundland *Privacy Act* RSNL 1990, c. P-22.~~

18. — On March 27, 2020 Zoom posted an entry on its blog, located on its website, admitting that the Zoom App was sending information to Facebook upon installation of the Zoom App and each time the Zoom App was opened. Zoom also admitted that the unauthorized disclosures began when Zoom contracted with Facebook to implement a “Login with Facebook” feature using Facebook’s proprietary “software development kit”.

19. — On March 27, 2020 Zoom released an updated version of the Zoom App which purported to no longer send unauthorized information regarding its users to Facebook. In order to obtain the purported increased security of the updated Zoom App, users must take the affirmative step of updating the Zoom App.

20. — Zoom did not take steps to block earlier versions of the App from accessing its videoconferencing platform to ensure that its users would download the updated version of the Zoom App.

21. — Zoom did not ensure that Facebook, or any other third party, took steps to delete Zoom users’ improperly collected private information.

The Proposed Class

22. — The plaintiff brings this action on his own behalf, and on behalf of a proposed class of individuals, (the “Class”) consisting of:

All Canadian residents whose personal information was collected and/or disclosed by Zoom to a third party upon installation or opening the Zoom videoconferencing application.

Part 2: RELIEF SOUGHT

1. The Plaintiff on behalf of the Class seeks, on his own behalf and on behalf of other Class Members:

- (a) An order pursuant to the *Class Proceedings Act*, RSBC 1996, c 50 certifying this action as a class proceeding and appointing the Plaintiff as the representative plaintiff for the national class;

- (b) Damages for:
- i. Negligence;
 - ii. ~~i.~~ Breach of contract (disgorgement or, in the alternative, expectation damages);
 - iii. ~~ii.~~ The tort of intrusion upon seclusion;
 - iv. ~~iii.~~ Breach of the *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, CCSM, c. P125; *The Privacy Act*, RSS 1978, c P-24; and *The Privacy Act* RSNL 1990, c. P-22;
 - v. The tort of breach of confidence; and
 - vi. Fraudulent, or alternatively, negligent misrepresentation;
- (b1) Restitution for unjust enrichment;
- (c) Damages pursuant to section 171 of the British Columbia *Business Practices and Consumer Protection Act*, S.B.C. 2004, c.2; section 13 of the Alberta *Consumer Protection Act*, R.S.A. 2000 c. C-26.3; section 8 93 of the Saskatchewan *The Consumer Protection and Business Practices Act*, S.S. 2013, c. C-30.2; section 23 of Manitoba's *The Business Practices Act*, CCSM c B120; sections 18 and 100 of the Ontario *Consumer Protection Act*, 2002, S.O. 2002, c. C-30, Sched. A; section 272 of the Quebec *Consumer Protection Act*, CQLR S.Q. c. P-40.1; section 4 of the Prince Edward Island *Business Practices Act*, c. B-7; section 15 of the *Consumer Product Warranty and Liability Act*, SNB 1978, c C-18.1; and section 10 of the Newfoundland *Consumer Protection and Business Practices Act*, S.N.L., 2009, c. C-31.1;
- (d) Special damages;
- (d1) An order, pursuant to s. 29 of the *Class Proceedings Act*, directing an aggregate assessment of damages;
- (d2) Costs of administering the plan of distribution;
- (e) Interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996 c. 79;

- (f) Costs of this action; and
- (g) Such further and other relief as this honourable court may deem meet.

Part 3: LEGAL BASIS

Statutory Torts for Breach of Privacy

1. Zoom's unauthorized disclosure to Facebook, Google, and other third parties of the plaintiff's and other Class Members' personal information and data, as set out in the whole of this claim, was in violation of the Privacy Policy and substantially, unreasonably, wilfully, and without claim of right violated the privacy of the plaintiff and other Class Members.

2. With respect to the plaintiff and other Class Members resident in British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador, Zoom's conduct constituted a tort pursuant to the *Privacy Act*, RSBC 1996, c 373; *The Privacy Act*, CCSM c P125; *The Privacy Act*, RSS 1978, c P-24; and *The Privacy Act*, RSNL 1990, c P-22. In each of these jurisdictions, Zoom's tort is actionable without proof of damage.

Negligence

3. Zoom owed a common law duty to the plaintiff and other Class Members to use reasonable care in the collection, storage, and retention of their personal information and data, and a duty to ensure that this information and data was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party.

4. ~~1.~~ At all material times Zoom knew, or ought to have known, it had a duty to protect the private information of its users.

5. ~~2.~~ At all material times Zoom knew, or ought to have known, it had a duty to fully disclose to its users the types of private information it collected from them, the purpose for which the private information was being collected, and the manner in which the private information was to be used by Zoom.

6. ~~3.~~ At all material times Zoom knew, or ought to have known, that it had a duty not to disclose private information concerning its users to third parties, including but not limited to Facebook and Google.

7. ~~4.~~ At all material times Zoom knew, or ought to have known, that it had a duty to clearly and robustly disclose to its users any and all unauthorized disclosure of the users' private information.

8. Particulars of Zoom's systemic breaches of duty, as set out in the whole of this claim, include:

- (a) failing to use reasonable care in the collection, storage, and retention of the the plaintiff's and other Class Members' personal information and data;
- (b) failing to ensure that the plaintiff's and other Class Members' personal information and data was safe, kept private, kept confidential, and protected and that it would not be subject to unauthorized disclosure to a third party;
- (c) failing to to protect the private information of the plaintiff and other Class Members;
- (d) failing to fully disclose to the plaintiff and other Class Members the types of private information and data it collected from them, the purpose for which the private information and data was being collected, and the manner in which the private information and data was to be used by Zoom;
- (e) disclosing the plaintiff's and other Class Members' private information and data to third parties, including but not limited to Facebook and Google, without Class Members' consent;
- (f) breaching the terms and requirements of the Privacy Policy;
- (g) failing to clearly and robustly disclose to the plaintiff and other Class Members any and all unauthorized disclosure of the users' private information;

- (h) failing to have appropriate and reasonable security procedures and organizational measures in place to protect the plaintiff's and other Class Members' personal information and data from unauthorized access, use or disclosure;
- (i) failing to disclose to the plaintiff and other Class Members that communications made over Zoom's videoconferencing services were not protected by end-to-end encryption, and misrepresenting to the plaintiff and other Class Members that they were;
- (j) misusing the personal information and data of the plaintiff and other Class Members;
and
- (k) failing to act in accordance with industry standards.

9. Zoom knew its practices were not in conformity with the Privacy Policy or with industry standards.

10. Zoom's conduct constituted a violation of privacy and a tort pursuant to the provisions of the *Privacy Act*, RSBC 1996, c 373; *The Privacy Act*, CCSM c P125; *The Privacy Act*, RSS 1978, c P-24; and *The Privacy Act*, RSNL 1990, c P-22. Zoom's statutory breaches are evidence that its conduct fell below the applicable standard of care.

11. Zoom's breaches of duty caused the plaintiff and other Class Members loss and damage, as particularized below.

12. The plaintiff and other Class Members are entitled to damages.

Intrusion upon seclusion

13. Zoom's unauthorized disclosure to Facebook, Google, and other third parties of the plaintiff's and other Class Members' personal information and data was intentional and reckless and, without lawful justification, invaded the private affairs and concerns of the plaintiff and other Class Members.

14. Zoom's recklessness amounted to intentional conduct. Zoom knew or ought to have known that its use of Facebook's SDK and the Firebase SDK would cause Zoom to disclose, without consent, the personal information and data of the plaintiff and other Class Members, contrary to the terms of its Privacy Policy. And Zoom knew or ought to have known that such conduct would intrude upon the private affairs and concerns of the plaintiff and other Class Members.

15. The information and data of the plaintiff and other Class Members that was disclosed by Zoom to Facebook, Google, and other third parties was — either independently or in the aggregate — inherently revealing and private, and a reasonable person would regard this invasion as highly offensive causing distress, humiliation, or anguish.

16. Zoom is liable for the tort of intrusion upon seclusion *vis-à-vis* the plaintiff and other Class Members.

17. The plaintiff and other Class Members are entitled to damages.

Breach of Confidence

18. The confidential information and data of the plaintiff and other Class Members, which they provided to Zoom in confidence, was misused by Zoom, to the detriment of the plaintiff and other Class Members and constituted the tort of breach of confidence.

19. The plaintiff and other Class Members relied on Zoom's commitment to privacy — as expressed in the Privacy Policy and as expressed in the E2E Representations and as mandated by legislation and industry standards. The plaintiff and other Class Members reasonably expected that their sensitive personal information and data would be kept by Zoom in confidence and not misused by Zoom for its own financial gain.

20. Contrary to this expectation, the plaintiff's and Class Members' confidential information and data was misused by Zoom to the detriment of the plaintiff and other Class Members. Zoom failed to take reasonable steps to protect the information and data, contrary to its stated commitments in the Privacy Policy and the E2E Representations and contrary to applicable legislation and industry standards.

21. As a consequence of Zoom's breach of confidence, the plaintiff and other Class Members are entitled to damages.

Breach of Contract

22. The plaintiff and other Class Members entered into identical or substantially similar contracts with Zoom for the use of Zoom's videoconferencing services.

23. When the plaintiff and other Class Members installed and opened the Zoom App or otherwise opened Zoom's videoconferencing services, they agreed — for good and valuable consideration — to allow Zoom to collect and retain their personal information and data. Zoom correspondingly agreed — for good and valuable consideration — to be bound by the Privacy Policy and ensure that the personal privacy of the plaintiff and other Class Members was protected in accordance with the Privacy Policy.

24. It was an express or implied term of the contracts that Zoom would have appropriate and reasonable security procedures and organizational measures in place to protect the plaintiff's and other Class Members' personal information and data from unauthorized access, use or disclosure.

25. It was an express or implied term of the contracts that Zoom would not disclose the plaintiff's and other Class Members' personal information and data to Facebook, Google, and other third parties, except as expressly stated in the Privacy Policy.

26. It was an express or implied term of the contracts that Zoom would comply with industry standards and ensure that its policies, procedures, and conduct complied with all applicable privacy legislation and all applicable consumer protection legislation.

27. It was also an express or implied term of the contracts that communications made through Zoom's videoconferencing services were protected by end-to-end encryption.

28. Zoom breached the terms of the contracts by failing to act in accordance with the terms of the Privacy Policy and, specifically, by:

- (a) failing to ensure that the personal privacy of the plaintiff and other Class Members was protected in accordance with the Privacy Policy;
- (b) disclosing the plaintiff's and other Class Members' personal information and data to Facebook, Google, and other third parties without their consent and contrary to the Privacy Policy;
- (c) failing to keep the personal information and data of the plaintiff and other Class Members confidential;
- (d) failing to have appropriate and reasonable security procedures and organizational measures in place to protect the plaintiff's and other Class Members' personal information and data from unauthorized access, use or disclosure;
- (e) misusing the personal information and data of the plaintiff and other Class Members;
- (f) failing to act in accordance with industry standards;
- (g) failing to protect communications made using Zoom's videoconferencing services with end-to-end encryption;
- (h) failing to act in accordance with applicable privacy legislation; and
- (i) failing to act in accordance with applicable consumer protection legislation.

29. As a consequence of Zoom's breach of the contracts, the plaintiff and other Class Members are entitled to expectation damages. In the alternative, Zoom should be required to disgorge its financial gains it realized from the breach of contracts.

5. ~~Zoom failed to meet the above noted duties to the Class and the Class alleges the tort of intrusion upon seclusion, and breach of the *Privacy Act*, R.S.B.C. 1996, c. 373; *Privacy Act*, CCSM, c.P125; *Privacy Act*, RSS 1978, c. P 24; and *Privacy Act* RSNL 1990, c. P 22.~~

Unjust Enrichment

30. Zoom used the “Login with Facebook” feature, the Firebase SDK, and the E2E Representations to attract new Zoom users — which it did. And in doing so, the price of Zoom’s stock increased, as did the value of Zoom generally.

31. Zoom received financial gain and was enriched from implementing the “Login with Facebook” feature, implementing the Firebase SDK, and making the E2E Representations while the plaintiff and other Class Members suffered a corresponding deprivation.

32. There was no juristic reason for Zoom’s enrichment and Class Members’ deprivation.

33. Class Members are entitled to restitution of Zoom’s financial gain.

Breach of Consumer Protection Legislation

British Columbia

34. With respect to the plaintiff and other Class Members resident in British Columbia who used Zoom’s videoconferencing services primarily for personal, family or household purposes:

- (a) the plaintiff and each Class Member was a “consumer”;
- (b) Zoom was a “supplier”;
- (c) Zoom’s videoconferencing services were a “service”; and
- (d) the supply of Zoom’s videoconferencing services from Zoom to the plaintiff and each Class Member was a “consumer transaction”;

all within the meaning of section 1 of the *Business Practices and Consumer Protection Act*, SBC 2004, c 2.

35. Zoom represented — in the Privacy Policy, in the E2E Representations, on the Zoom App, on Zoom’s website, and on Zoom’s blog — that it was committed to protecting the personal information and data that Class Members shared with Zoom, and that Zoom would protect Class

Members' personal information and data from unauthorized access, use, or disclosure. Specific representations made by Zoom in the context of consumer transactions with the plaintiff and other Class Members include:

- (a) Zoom takes users' privacy extremely seriously;
- (b) Zoom does not sell its users' data;
- (c) Zoom has never sold user data in the past or has no intention of selling users' data going forward;
- (d) Zoom complies with all applicable privacy laws, rules, and regulations in the jurisdictions within which it operates;
- (e) Zoom collects only the data from individuals using Zoom platform required to provide the service and ensure they are delivered effectively under a wide variety of settings in which its users may be operating (and this data includes basic technical information, such as the user's IP address, OS details, and device details);
- (f) Zoom does not mine user data or sell user data of any kind to anyone;
- (g) Zoom would only collect, use, and disclose its users' personal information lawfully and responsibly;
- (h) Zoom works to ensure that its users' personal information is kept confidential while in its care;
- (i) Zoom is accountable to protect and safeguard the personal information it collects, uses, and discloses;
- (j) Zoom ensures that current privacy policies and procedures are compliant and established with privacy legislation;
- (k) Zoom takes security measures to ensure personal information is protected from loss, theft, unauthorized access, use, copying, or disclosure;

- (l) Zoom reviews and updates its security measures to meet industry standards;
- (m) Zoom protects communications made using its videoconferencing services with end-to-end encryption;
- (n) Protecting the privacy and security of user information is essential and fundamental to Zooms' values and the way it does business; and
- (l) Zoom has privacy policies and practices in place that meet the requirements of the rules and regulations.

36. Zoom's representations, including the E2E Representations, were relied on by the plaintiff and other Class Members in connection with the consumer transactions when they decided to use Zoom's videoconferencing services primarily for personal, family or household purposes.

37. Zoom's representations, including the E2E Representations, were calculated or would naturally tend to induce the plaintiff and other Class Members to act on them.

38. Contrary to Zoom's other representations and as set out in the whole of this claim, Zoom # disclosed the plaintiff's and other Class Members' personal information and data to Facebook, Google, and other third parties without their consent. Zoom's representations were false, misleading, and untrue and constituted a "deceptive act or practice" within the meaning of section 4 and contrary to section 5 of the *Business Practices and Consumer Protection Act*.

39. Further and contrary to Zoom's representations, particularly the E2E Representations, and as set out in the whole of this claim, Zoom did not — at all material times — protect communications made using its videoconferencing services with end-to-end encryption.

40. The plaintiff and other Class Members are entitled to statutory damages under section 171 of the *Business Practices and Consumer Protection Act*.

Alberta

41. With respect to Class Members resident in Alberta who used Zoom's videoconferencing services primarily for personal, family or household purposes:

- (a) each Class Member was a “consumer”;
- (b) Zoom was a “supplier”;
- (c) Zoom’s videoconferencing services were a “service”; and
- (d) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer transaction”;

all within the meaning of section 1 of the *Consumer Protection Act*, RSA 2000, c C-26.3.

42. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services primarily for personal, family or household purposes.

43. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false, misleading, and deceptive and constituted an “unfair practice” within the meaning of and contrary to section 6 of the *Consumer Protection Act*.

44. Class Members are entitled to statutory damages under section 13 of the *Consumer Protection Act*.

Saskatchewan

45. With respect to Class Members resident in Saskatchewan who used Zoom’s videoconferencing services ordinarily for personal, family or household purposes:

- (a) each Class Member was a “consumer”;
- (b) Zoom was a “supplier”; and
- (c) Zoom’s videoconferencing services were a “service”;

all within the meaning of section 2 of *The Consumer Protection and Business Practices Act*, SS 2013, c C-30.2.

46. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services ordinarily for personal, family or household purposes.

47. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false, misleading, and deceptive and constituted an “unfair practice” within the meaning of sections 4 and 6 and contrary to section 8 of *The Consumer Protection and Business Practices Act*.

48. Class Members are entitled to statutory damages under section 93 of *The Consumer Protection and Business Practices Act*.

Manitoba

49. With respect to Class Members resident in Manitoba who used Zoom’s videoconferencing services primarily for personal, family or household use:

- (a) each Class Member was a “consumer”;
- (b) Zoom was a “supplier”;
- (c) Zoom’s videoconferencing services were “goods”; and
- (d) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer transaction”;

all within the meaning of section 1 of *The Business Practices Act*, CCSM c B120.

50. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services primarily for personal, family or household use.

51. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false, misleading, and deceptive and constituted an “unfair business practice” within the meaning of sections 1 and 2 and contrary to section 5 of *The Business Practices Act*.

52. Class Members are entitled to statutory damages under section 23 of *The Business Practices Act*.

Ontario

53. With respect to Class Members resident in Ontario who used Zoom’s videoconferencing services for personal, family or household purposes:

- (a) each Class Member was a “consumer”;
- (b) Zoom was a “supplier”;
- (c) Zoom’s videoconferencing services were a “service”;
- (d) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer transaction”; and
- (e) Zoom and Class Members entered into a “consumer agreement” with respect to the supply of Zoom’s videoconferencing services;

all within the meaning of section 1 of the *Consumer Protection Act, 2002*, SO 2002, c 30, Sch A.

54. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services for personal, family or household purposes.

55. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false,

misleading, and deceptive and constituted an “unfair practice” within the meaning of section 14 and contrary to section 17 of the *Consumer Protection Act, 2002*.

56. Class Members are entitled to statutory damages under sections 18 and 100 of the *Consumer Protection Act, 2002*.

Quebec

57. With respect to Class Members resident in Quebec:

(a) each Class Member was a “consumer”; and

(b) Zoom was a “merchant”;

all within the meaning of section 1 of the *Consumer Protection Act, CQLR c P-40.1*.

58. As set out above and in the whole of this claim, a contract for services was entered into, in the course of Zoom’s business, between each Class Member in Quebec and Zoom, within the meaning of section 2 of the *Consumer Protection Act*.

59. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members when entering into contracts with Zoom for videoconferencing services.

60. As set out above and in the whole of this claim, Zoom acted contrary to those representations. The representations — including the E2E Representations — made by Zoom to Class Members in Quebec were false and misleading and, accordingly, Zoom contravened section 219 of the *Consumer Protection Act*.

61. Class Members are entitled to statutory damages under section 272 of the *Consumer Protection Act*.

Prince Edward Island

62. With respect to Class Members resident in Prince Edward Island who used Zoom’s videoconferencing services for personal, family or household purposes:

- (a) each Class Member was a “consumer”;
- (b) Zoom’s videoconferencing services were “services”; and
- (c) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer transaction”;

all within the meaning of section 1 of the *Business Practices Act*, RSPEI 1988, c B-7.

63. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services for personal, family or household purposes.

64. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false, misleading, and deceptive and constituted an “unfair practice” within the meaning of section 2 and contrary to section 3 of the *Business Practices Act*.

65. Class Members are entitled to statutory damages under section 4 of the *Business Practices Act*.

New Brunswick

66. With respect to Class Members resident in New Brunswick who used Zoom’s videoconferencing services for personal, family or household purposes:

- (a) each Class Member was a “buyer”;
- (b) Zoom was a “seller”; and
- (c) Zoom’s videoconferencing services were a “consumer product”;

all within the meaning of section 1 of the *Consumer Product Warranty and Liability Act*, SNB 1978, c C-18.1.

67. As set out above and in the whole of this claim, a contract for the supply of a consumer product was entered into, in the course of Zoom’s business, between each Class Member in New Brunswick and Zoom, within the meaning of section 1 of the *Consumer Product Warranty and Liability Act*.

68. As set out above and in the whole of this claim, Zoom made various statements — including the E2E Representations — which were relied on, or reasonably relied on, by Class Members as warranties under section 4 of the *Consumer Product Warranty and Liability Act*.

69. As set out above and in the whole of this claim, Zoom’s statements — including the E2E Representations — were false and misleading, and Zoom acted contrary to those warranties.

70. Class Members are entitled to statutory damages under section 15 of the *Consumer Product Warranty and Liability Act*.

Nova Scotia

71. With respect to Class Members resident in Nova Scotia who used Zoom’s videoconferencing services for personal, family or household purposes:

- (a) each Class Member was a “purchaser”; and
- (b) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer sale”;

all within the meaning of section 26 of the *Consumer Protection Act*, RSNS 1989, c 92.

72. As set out above and in the whole of this claim, a contract for the supply of a contract of sale of goods or services was entered into, in the course of Zoom’s business, between each Class Member in Nova Scotia and Zoom.

73. As set out above and in the whole of this claim, Zoom made various statements — including the E2E Representations — which were relied on, or reasonably relied on, by Class Members as conditions or warranties under section 26 of the *Consumer Protection Act*.

74. As set out above and in the whole of this claim, Zoom’s statements — including the E2E Representations — were false and misleading, and Zoom acted contrary to those conditions or warranties.

75. As set out above, Class Members are entitled to damages at common law for breach of conditions or warranties under section 26 of the *Consumer Protection Act*.

Newfoundland and Labrador

76. With respect to Class Members resident in Newfoundland and Labrador who used Zoom’s videoconferencing services for personal, family or household purposes:

- (a) each Class Member was a “consumer”;
- (b) Zoom was a “supplier”;
- (c) Zoom’s videoconferencing services were “services”; and
- (d) the supply of Zoom’s videoconferencing services from Zoom to each Class Member was a “consumer transaction”; and

all within the meaning of section 2 of the *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1.

77. As set out above and in the whole of this claim, Zoom made various representations — including the E2E Representations — which were relied on by Class Members in connection with the consumer transactions when they decided to use Zoom’s videoconferencing services for personal, family or household purposes.

78. As set out above and in the whole of this claim, Zoom acted contrary to those representations. Zoom’s representations — including the E2E Representations — were false, misleading, and deceptive and constituted an “unfair business practice” within the meaning of section 7 and contrary to section 9 of the *Consumer Protection and Business Practices Act*.

79. Class Members are entitled to statutory damages under section 10 of the *Consumer Protection and Business Practices Act*.

Misrepresentation

80. As set out above and in the whole of the claim, particularly relating to the E2E Representations, Zoom represented to the plaintiff and other Class Members that communications made using its videoconferencing services were protected by end-to-end encryption, when such communications were not, in fact, protected by end-to-end encryption.

81. Zoom made the E2E Representations knowing they were false, without belief in their truth, or reckless as to whether they were true or false.

82. The E2E Representations were relied on by the plaintiff and other Class Members when they decided to use Zoom's videoconferencing services, resulting in loss.

83. Zoom intended the plaintiff and other Class Members to act on the E2E Representations, and Zoom is liable for the tort of fraudulent misrepresentation.

84. Further, or in the alternative:

- a. Zoom owed a duty of care to the plaintiff and other Class Members;
- b. the representations set out above and in the whole of the claim, particularly the E2E Representations, were untrue, inaccurate, or misleading;
- c. Zoom was negligent in making these representations, particularly the E2E Representations;
- d. the plaintiff and other Class Members reasonably relied on these representations, particularly the E2E Representations; and
- e. as a result of which, the plaintiff and other Class Members suffered damages.

85. Consequently, Zoom is liable to the plaintiff and other Class Members for negligent misrepresentation.

6. — Additionally, at all material times Zoom knew, or ought to have known, it had a duty to not to engage in a “deceptive act or practice”, an “unfair practice”, an “unfair business practice”, or make a “false or misleading representation”, and the plaintiff pleads the provisions of the ~~British Columbia Business Practices and Consumer Protection Act, S.B.C.~~; the ~~Alberta Consumer Protection Act, R.S.A. 2000 c. C-26.3~~; the ~~Saskatchewan Consumer Protection and Business Practices Act, S.S. 2013, c. C-30.2~~; the ~~Ontario Consumer Protection Act, 2002, S.O. 2002, c. C-30, Sched. A~~; the ~~Quebec Consumer Protection Act, S.Q. c. P-40.1~~; and the ~~Newfoundland Consumer Protection and Business Practices Act, S.N.L., 2009, c. C-31.1e.2.~~

Legislation

86. 7. The Plaintiff pleads and relies on: the Class Proceeding Act, RSBC 1996, c. 34.

- (a) Business Practices and Consumer Protection Act, SBC 2004, c 2;
- (b) Class Proceeding Act, RSBC 1996, c 34;
- (c) Consumer Protection Act, 2002, SO 2002, c 30, Sch A;
- (d) Consumer Protection Act, CQLR c P-40.1;
- (e) Consumer Protection Act, RSA 2000, c C-26.3;
- (f) Consumer Protection and Business Practices Act, SNL 2009, c C-31.1;
- (g) Court Jurisdiction and Proceedings Transfer Act, RSBC 2003, c 28;
- (h) Court Order Interest Act, RSBC 1996 c 79;
- (i) Privacy Act, RSBC 1996, c 373;
- (j) The Business Practices Act, CCSM c B120;
- (k) Business Practices Act, RSPEI 1988, c B-7;
- (l) The Consumer Protection and Business Practices Act, SS 2013, c C-30.2;

- (m) Consumer Protection Act, RSNS 1989, c 92;
- (n) Consumer Product Warranty and Liability Act, SNB 1978, c C-18.1;
- (o) The Privacy Act, CCSM c P125;
- (p) The Privacy Act, RSNL 1990, c P-22; and
- (q) The Privacy Act, RSS 1978, c P-24.


Plaintiff's address for service: Collette Parsons Corrin LLP
1750-700 West Georgia Street
Vancouver, B.C. V7Y 1B6

Murphy Battista LLP
2020 – 650 West Georgia Street
Vancouver, BC V6B 4N7

Place of trial: Vancouver, British Columbia,

The address of the registry is: 800 Smithe Street, Vancouver, BC, V6Z 2E1

Date: ~~April 6, 2020, January 24, 2023~~
April 28, 2023



Signature of [X] lawyer for plaintiff
A. C. Richard Parsons

Rule 7-1(1) of the Supreme Court Civil Rules states:

- (2) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
 - (a) prepare a list of documents in Form 22 that lists
 - (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
 - (ii) all other documents to which the party intends to refer at trial, and
 - (b) serve the list on all parties of record.

**ENDORSEMENT ON ORIGINATING PLEADING OR PETITION
FOR SERVICE OUTSIDE BRITISH COLUMBIA**

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding and the plaintiff and the Class plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act* RSBC 2003 Ch 28 (the "CJPTA") in respect of the defendant, Zoom. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to section 10 of the CJPTA because this proceeding:

(e) concerns contractual obligations, and

(i) the contractual obligations, to a substantial extent, were to be performed in British Columbia;

(f) concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia

APPENDIX

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

The Defendant disclosed private information belonging to the plaintiff and members of the proposed class and failed to have end-to-end encryption in breach of the relevant privacy acts and consumer protection acts across Canada and in breach of its obligations pursuant to the tort of intrusion upon seclusion. The Defendant's conduct also constituted breach of confidence, negligence, and fraudulent or negligent misrepresentation, and the Defendant was unjustly enriched by its conduct.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

- a motor vehicle accident
- medical malpractice
- another cause

A dispute concerning:

- contaminated sites
- construction defects
- real property (real estate)
- personal property
- the provision of goods or services or other general commercial matters
- investment losses
- the lending of money
- an employment relationship
- a will or other issues concerning the probate of an estate
- a matter not listed here

Part 3: THIS CLAIM INVOLVES:

- a class action
- maritime law
- aboriginal law
- constitutional law
- conflict of laws
- none of the above
- do not know

Part 4: ENACTMENTS RELIED ON

1. ~~*Business Practices and Consumer Protection Act*, S.B.C. c.2.~~
2. ~~*Class Proceedings Act* R.S.B.C. 1996, c. 50~~
3. ~~*Consumer Protection Act*, R.S.A. 2000 c. C-26.3~~
4. ~~*Consumer Protection and Business Practices Act*, S.S. 2013, c. C-30.2~~
5. ~~*Consumer Protection Act*, 2002, S.O. 2002~~
6. ~~*Consumer Protection Act*, S.Q. c. P-40.1~~
7. ~~*Consumer Protection and Business Practices Act*, S.N.L., 2009, c. C-31.1~~
8. ~~*Court Order Interest Act*. R.S.B.C. 1996 c.79.~~
9. ~~*Privacy Act*, R.S.B.C. 1996, c. 373.~~
10. ~~*Privacy Act*, CCSM, c.P125~~
11. ~~*Privacy Act*, RSS 1978, c. P-24~~
12. ~~*Privacy Act* RSNL 1990, c. P-22~~

1. *Business Practices and Consumer Protection Act*, SBC 2004, c 2;
2. *Class Proceeding Act*, RSBC 1996, c 34;
3. *Consumer Protection Act*, 2002, SO 2002, c C-30, Sch A;
4. *Consumer Protection Act*, CQLR c P-40.1;
5. *Consumer Protection Act*, RSA 2000, c C-26.3;
6. *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1;
7. *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c 28;
8. *Court Order Interest Act*, RSBC 1996 c 79;
9. *Privacy Act*, RSBC 1996, c 373;
10. *The Business Practices Act*, CCSM c B120;
11. *Business Practices Act*, RSPEI 1988, c B-7;
12. *The Consumer Protection and Business Practices Act*, SS 2013, c C-30.2;
13. *Consumer Protection Act*, RSNS 1989, c 92;
14. *Consumer Product Warranty and Liability Act*, SNB 1978, c C-18.1;
15. *The Privacy Act*, CCSM c P125;
16. *The Privacy Act*, RSNL 1990, c P-22; and
17. *The Privacy Act*, RSS 1978, c P-24.