No. S-246757
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

Between

[redacted] STEEVES

PLAINTIFF

and

WHALECO CANADA INC. doing business as TEMU,
WHALECO INC. doing business as TEMU and
PDD HOLDINGS INC. formerly known as PINDUODUO INC.

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

NOTICE OF CIVIL CLAIM

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.

THE PLAINTIFF'S CLAIM

PART 1: STATEMENT OF FACTS

Overview

1. The Plaintiff wishes to institute a class action on behalf of the following class, of which she is a member, namely:

> All persons resident in Canada, excluding Quebec, who used the Temu platform, or had electronic communications with Temu users, or who had their data stored on devices used by Temu users, or any other group to be determined by the Court.

2. Temu is an online marketplace operated by the Defendants that offers heavily discounted consumer goods that are mostly shipped directly from China.

3. The Plaintiff contends that the Defendants have been and continue to collect, compile, store, and/or disseminate user data exceeding that which is necessary for online shopping applications such as Temu, deploying a sophisticated arsenal of tools exfiltrating the totality of private data contained on a user's device.

4. The intentional and excessive collection of personal user data extends to biometric information such as facial characteristics, fingerprints and voiceprints, and to users' precise geospatial location. The Temu platform allows the Defendants to conduct surreptitious

surveillance of app users by bypassing users' phones' security systems and enabling the Defendants to access and read users' private messages, track notifications, gain access to the passwords, calendars, contacts, pictures, cameras and microphones on users' phones make changes to the settings on users' phones, and obtain system information and phone serial (MAC) numbers. Activity on other apps operating on users' devices are also tracked.

5. The Defendants' intentional, excessive, surreptitious, and grossly disproportionate collection of personal information has been and continues to be facilitated, furthered or otherwise advanced by their practice of insufficiently disclosing to actual and prospective users the nature, level, extent and quantity of data collected through the Temu platform.

6. The Defendants' practice of deceptive and misrepresentational disclosure prevents Temu users from effectively consenting to the Defendants' collection of their data and from ascertaining the manner their personal information is used by the Defendants.

7. As Temu is a Chinese-owned company operated by a cadre of former Chinese Communist Party officials, the violations of Temu users' privacy rights are compounded by the Defendants' exposure of Temu users' personal information to misappropriation or compelled disclosure by individuals and entities part of, or affiliated with, the Chinese Communist Party and/or People's Republic of China.

8. The Defendants' deliberate and clandestine practices intentionally invade Class Members' privacy in order to enrich themselves as Class Members' expense and otherwise harm Class Members.

9. The Defendants' unlawful acts violated and continue to violate the *Privacy Act*, R.S.B.C. 1996, c. 373. Through this class action, Canadians (outside Quebec) seek to hold the Defendants accountable for this unlawful misconduct.

The Parties

10. Defendant Whaleco Canada Inc. ("Temu Canada") is a Canadian corporation with its head office in Victoria, British Columbia. Temu Canada carries on business in Canada, including in British Columbia, by making the Temu app available and selling products to Canadian users.

11. Defendant Whaleco Inc. ("Temu") is an American corporation with its head office in Boston, Massachusetts. It is an online marketplace offering heavily discounted goods mostly shipped to consumers directly from China that is operated by Defendant PDD Holdings Inc. Temu carries on business worldwide, including in British Columbia and Canada, by making the Temu app available and selling products to Canadian users.

12. Temu handles delivery, promotion and after sales services for merchants through its platform, which includes over 80,000 suppliers. In 2023, Temu was the most downloaded app in the United States, with users reportedly spending close to twice the amount of time on the app than on Amazon.

13. Defendant PDD Holdings Inc. ("PDD") is a Chinese e-commerce company founded in 2015 under the name Pinduoduo Inc. In February 2023, PDD Holdings claims to have relocated its "principal executive offices" from Shanghai, China to Dublin, Ireland. PDD however maintains the overwhelming majority of its operations in China, including by way of several subsidiaries located therein. PDD Holdings owns the company that operates the Temu online marketplace, namely, the Defendant Whaleco Inc. PDD carries on business worldwide, including in British Columbia and Canada, by making the Temu app available and selling products to Canadian users.

14. Defendants PDD and Temu operate as corporate alter egos that are neither separate nor independent. Temu is directly controlled by Defendant PDD, which directs Temu's operations and corporate policies. The same is true as concerns Temu Canada, a subsidiary of Temu that is also ultimately controlled by Defendant PDD. Each of the Defendants was an agent of the other for the purposes of developing, distributing, and operating the Temu app. All the Defendants participated in the provision of the Temu app to users in Canada

and engaged in the surveillance and other invasions of privacy addressed herein. The precise roles of each of the Defendants are well known to them.

15. The Plaintiff is a resident of British Columbia. At all times relevant to the present class action, they were a user of the Temu app. The Plaintiff downloaded the Temu app onto her phone sometime in 2023 and has since made several product purchases using her credit card that were later delivered to her.

16. At all material times after downloading the app, the Plaintiff continued to engage telephone conversations, text message exchanges, and other communications with friends, family, and others, on her cellular phone, and also stored pictures, and other media on her phone containing her personal information and the personal information of others with whom she had exchanges using the said phone.

17. Among other purchases made by the Plaintiff are purchase transactions completed on the Temu app for which orders were delivered on May 26, June 5, September 6, 19, 20, and 29, October 11, 18, and 27, November 28, and December 8 and 13, 2023, and on September 9, 11, 12, and 17, 2024. This includes orders for which refunds were requested and issued on September 14, 19, and 27 and October 3, 2023 and August 30, 2024.

18. The Plaintiff's phones, a Motorola Moto G and TCL 20 Pro do not have an option allowing for the user to set permissions for downloaded apps to access the camera or contacts stored on the phone.

19. Until the public revelations of Temu's misconduct, the Plaintiff was unaware that the Defendants were and continue to be engaged in collecting, compiling, storing, and/or dissemination of user data and conducting surveillance of users' phones and personal data.

20. The Plaintiff brings this claim on her own behalf and on behalf of all individuals in Canada, other than Excluded Persons and residents of Quebec, who used the Temu app, had electronic communications with Temu users, or had their data stored on devices used by

Temu users from the date Temu began engaged in the aforementioned unlawful practices until the date this action is certified as a class proceeding ("**Class**", "**Class Members**" and "**Class Period**").

21. Excluded Persons means: (1) Directors and officers of Temu and their immediate families; and (2) Counsel for the parties, and the case management judge and trial judge in this proceeding, and their immediate families.

Background

22. PDD launched its new initiative, Temu, in September 2022. PDD developed the Temu app to be a global version of its precursor app, Pinduoduo, with the United States as its principal market.

23. Significant concerns were raised regarding the Pinduoduo app, which was removed from the Google Play Store due to the presence of malware exploiting vulnerabilities in the Android operating system.

24. More specifically, the malware was spying on users and competitors through as many as 83 permissions, including access to biometrics (such as fingerprints), Bluetooth, and Wi-Fi network information.

25. Temu operates similarly, although it only asked for 24 permissions, including access to Bluetooth, biometric data, and Wi-Fi network information. On April 3, 2023, CNN reported that multiple cybersecurity teams found sophisticated malware on Pinduoduo's mobile app for Google Android devices. The malware enabled the Pinduoduo app to bypass user security permissions and malware detection capabilities and access private messages, change settings, view data from other apps, and prevent uninstallation. The investigation followed Google's suspension of the app from the Google Play store on March 21, 2023.

26. Also in April 2023, the U.S.-China Economic and Security Review Commission, a governmental entity established to investigate, assess and report on the national security implications of the economic relationship between the U.S. and China, issued a brief noting the significant data risks associated with the Temu app.

27. The brief highlights that the majority of engineers who developed Pinduoduo were transferred to work for Temu following the former's suspension from the Google Play store.

28. Analysts who authored a Grizzly Research Report concluded that the Pinduoduo app was secretly collecting personal and private information from users without their knowledge or consent including highly-sensitive biometric data contained on users' devices. The Report is entitled "We Believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests" dated September 6, 2023.

29. These analysts also concluded that many of the problems with the Pinduoduo app were equally present with the Temu app. More recently, Apple suspended the Temu app from the Apple App Store due to Temu not being in compliance with Apple's data privacy standards and making misrepresentations concerning the types of data the app can access and collect from users, including how it collects and uses that data.

30. Politico investigated the matter and concluded: "Apple said Temu previously violated the company's mandatory privacy rules. It said it had found that Temu misled people about how it uses their data. Temu's so-called privacy nutrition labels — descriptions about the types of data an app can access, how it does so and what it uses them for — did not accurately reflect its privacy policy, said Apple. Temu also isn't letting users choose not to be tracked on the internet."

31. Because of these concerns with the Temu app, the state of Montana has banned it from being installed on government devices – the issue being that it provides "personal information or data to foreign adversaries" and is "dangerous" since it bypasses phone

security systems to read a user's private messages, makes changes to the phone's settings and track notifications.

32. On December 20, 2023, the United States House of Representatives' Committee on Energy and Commerce sent Temu a letter demanding information relating to the data collection practices with respect to the Pinduoduo and Temu apps and expressing concerns about the amount of data collected from consumers.

33. The Committee's letter also highlighted that "Temu's business model is not profitable" and that "[its] decision to operate at a loss makes one question the intentions of the app, especially when Temu's parent company's app, Pinduoduo, was suspended by Google over malware concerns."

34. The Committee's letter contains eighteen (18) questions to be answered by the Defendants, in addition to sub-questions, with a total of eleven (11) concerning Temu's data collection, retention, and disclosure practices, and associations and interactions with the Chinese Communist Party. Note that the Committee's investigation into Temu's practices is ongoing.

35. The Grizzly Report further revealed that the scope of the data collected by Temu goes well beyond the scope of data that is necessary in order to run an online shopping app. It has been recommended to remove the Temu app from users phone in order to prevent it from its covert information theft.

36. The analysts concluded that the "TEMU app is purposefully and intentionally loaded with tools to execute virulent and dangerous malware and spyware activities on user devices which have downloaded and installed the TEMU app" suggesting that Defendant PDD is a "fraudulent company" and that "its shopping app Temu is cleverly hidden spyware that poses an urgent security threat to U.S. national interests."

37. Even more concerning is that the Grizzly Research Report concludes that there is "smoking gun evidence" that "Temu is the most dangerous malware/spyware package currently in widespread circulation."

38. The main findings in the Report are the following:

(a) "The app has hidden functions that allow for extensive data exfiltration unbeknown to users, potentially giving bad actors full access to almost all data on customers' mobile devices."

(b) "It is evident that great efforts were taken to intentionally hide the malicious intent and intrusiveness of the software."

(c) "We engaged numerous independent data security experts to decompile and analyze TEMU app's code, integrated with experts of our own staff, and analysts who have written independently in the public domain."

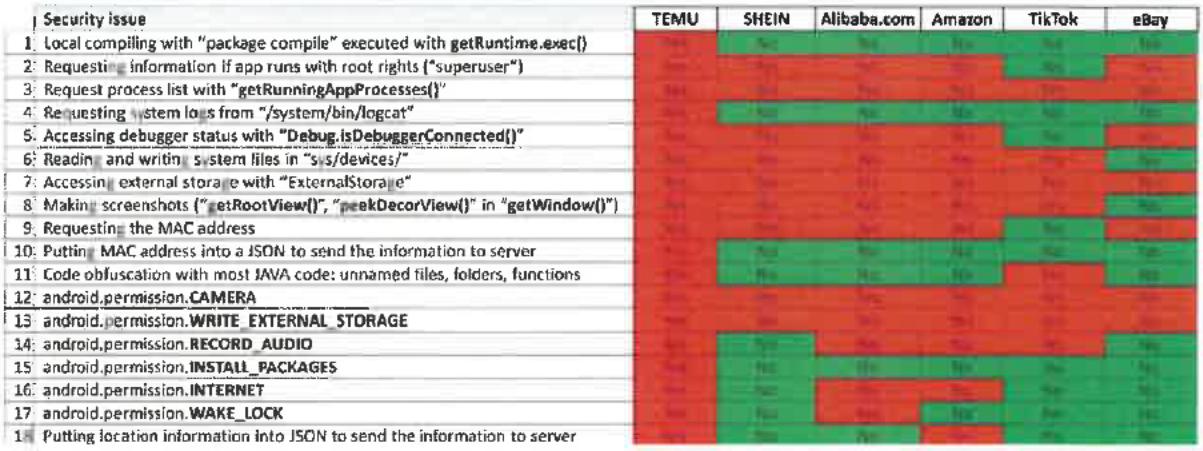
(d) "Contributing to the danger of mass data exfiltration is the fast uptake rate of the TEMU app: over 100 million app downloads in the last 9 months, all in U.S. and Europe. TEMU is not offered in China."

(e) "The TEMU app development team includes 100 engineers who built the Pinduoduo app, which earned a suspension from the Google Play Store."

(f) "Pinduoduo app got reinstated by removing the 'bad parts,' some of which were identically utilized as components of the TEMU app, strongly indicating malicious intent."

(g) "We strongly suspect that TEMU is already, or intends to, illegally sell stolen data from Western country customers to sustain a business model that is otherwise doomed for failure."

39. The software functions that Temu uses as compared to other comparable shopping apps is concerning and inappropriate and excessive, as depicted in the below chart:



	Security issue	TEMU	SHEIN	Alibaba.com	Amazon	TikTok	eBay
1	Local compiling with "package compile" executed with **getRuntime.exec()**						
2	Requesting information if app runs with root rights ("superuser")						
3	Request process list with "**getRunningAppProcesses()**"						
4	Requesting system logs from "/system/bin/logcat"						
5	Accessing debugger status with "**Debug.isDebuggerConnected()**"						
6	Reading and writing system files in "sys/devices/"						
7	Accessing external storage with "ExternalStorage"						
8	Making screenshots ("**getRootView()**", "**peekDecorView()**" in "**getWindow()**")						
9	Requesting the MAC address						
10	Putting MAC address into a JSON to send the information to server						
11	Code obfuscation with most JAVA code: unnamed files, folders, functions						
12	android.permission.**CAMERA**						
13	android.permission.**WRITE_EXTERNAL_STORAGE**						
14	android.permission.**RECORD_AUDIO**						
15	android.permission.**INSTALL_PACKAGES**						
16	android.permission.**INTERNET**						
17	android.permission.**WAKE_LOCK**						
18	Putting location information into JSON to send the information to server						

40. It was reported in the United Kingdom that "law enforcement authorities have issued a stark warning about this online marketplace. They have uncovered evidence of the app harvesting customer data and expressed concerns that this data may find its way into Chinese hands", a copy of the Cybersecurity Insiders article entitled "China Temu App caused data privacy concerns in United Kingdom".

41. The Temu app was intentionally designed to hide the malicious features to prevent users from discovering the data privacy violations.

42. The Defendants make the following representations on Temu's website:

- "Temu is a safe shopping website. We care about our customers' privacy and data security."

- "Our Commitment to Your Privacy

1. Transparent Data Usage: Our Privacy Policy details how we collect and use your information.

2. No Unnecessary Data Sharing: We do not share your personal information with third-party merchandise partners on Temu, ensuring your data remains confidential and secure.

3. Customer Consent and Control: You have control over your personal information. We seek your consent for any data processing and provide options to manage your privacy settings."

- "Ensuring a Safe Shopping Experience Shopping on Temu is not just about finding great deals; it's also about feeling secure and protected. We continuously evolve our security measures to ensure that you can shop with confidence, knowing your data and other information are safe with us."

43. These representations are part of the Privacy Policy available on www.temu.com.

44. Despite the Defendants' assurances, the Temu app contains "self-compiling software" that circumvents your phone's malware detection abilities and allows the Defendants to illegally steal user data.

45. In addition, and without limiting the generality of the foregoing or of what follows, the in-app browser in the Temu app inserts JavaScript code into the websites visited by Temu users to track every detail about Temu users' website activity. This has enabled Temu to secretly and invasively accumulate massive amounts of highly private and sensitive personal information and data by tracking their activities on third-party websites.

46. As well, on August 15, 2024, a coalition of Attorneys General of 21 states wrote a letter to Mr. Qin Sun, President of Temu/WhaleCo. Inc and Mr. Chen Lei, CEO of PDD Holdings Inc. "demanding answers… regarding [Temu's] alleged ties with the Chinese Communist Party (CCP), data collection and sharing practices, and possible violations of the Uyghur Forced Labor Prevention Act (UFLPA)."

47. Owing to the opacity and duplicity of Temu's data and information collection, retention, and disclosure practices, the Attorneys Generals' letter demands that Temu answer a series of questions contained therein, including the following:

a. Does Temu or PDD Holdings collect U.S. consumer data? If so, please explain the type of data collected from U.S. consumers, including but not limited to data regarding consumer preferences, biometric data, political leanings, health data, race, religion, or sex. Please explain the rationale for the different types of data

collected and the manner in which you notify consumers of the type of data collected.

b. How is U.S. consumer data retained and stored? Please provide documentation of Temu's or PDD Holdings' cybersecurity and data retention and storage policies for U.S. consumer data. What security measures are in place to prevent unauthorized third parties from accessing U.S. consumer data acquired or retained by Temu?

c. Has the CCP [note: Chinese Communist Party], or any of its officials, members, or affiliates, required or requested that Temu or PDD Holdings turn over any data collected on U.S. citizens? If so, please state how many directives or requests you received and explain what data was requested and whether any (or all) data was turned over to the CCP.

d. What consumer data does Temu or PDD Holdings retain when an individual consumer request their data be deleted, or their account deactivated?

e. Does Temu or PDD Holdings sell U.S. consumer data? If so, who does Temu or PDD Holdings sell that consumer data to, and are any measures employed to safeguard the identities of U.S. consumers? What percentage of [Temu's and/or PDD's] profits are attributable to retail sales, and what percentage of profits attributable to data sold to third parties?

f. Various reports indicate that several former CCP members are on PDD Holdings' executive leadership team. Do these members have access to any U.S. consumer data possessed or acquired by Temu? If so, please explain the nature of the members' access to that data.

g. CNN reports that Temu's sister app (Pinduoduo), also owned by PDD Holdings, was removed from Google Play in 2023 after experts discovered malware that could be used to spy on users. Did the same app developer create the Temu app? Please explain in detail all measures Temu has taken in the past and any measures currently being employed to ensure the app is free of malware or any other programs that would allow Temu or anyone else to spy on U.S. users.

48. The Attorneys General's requests that Temu and PDD include "any documents relied on to answer these questions" in addition to the actual responses, which became due on September 15, 2024. It is unknown at the time of preparing the present Notice of Civil Claim whether Temu has complied with the Attorneys General's requests, in whole or in part, whether on the due date, or otherwise.

49. The Attorneys General's letter further highlighted their willingness to "consider all available measures to protect [their] citizens" from Temu's "harmful business practices… [i]f uncorrected…"

50. The Defendants have disputed claims that the personal data and information collected and retained from users is collected by on or behalf of, or otherwise disclosed, voluntarily or otherwise, to the Chinese Communist Party.

51. However, as highlighted in the letter sent to the Defendants by the U.S. House Committee on Energy and Commerce in December 2023:

> From 2014 to 2017, the Chinese Communist Party (CCP) passed several laws requiring all Chinese tech companies to allow CCP officials access to user data. Further, all Chinese tech companies must comply with the demands of the CCP, which in some cases is a "require[ment] to build [their] networks in such a way as where the Chinese government has access." Past violations by TikTok, and other Chinese-owned applications, to protect user data, and China's record of accessing Americans' information, undercuts any claim of data security.[1]

52. China's Cybersecurity Law further obligates Critical Information Infrastructure operators to provide the government with unobstructed access to their data, including on demand, and also mandates that the data be stored exclusively within mainland China.

53. On June 25, 2024, the Attorney General of Arkansas filed a lawsuit against PDD Holdings Inc. and WhaleCo Inc. in respect of violations of the *Arkansas Deceptive Trade Practice Act* and the *Arkansas Personal Information Protection Act.* The accompanying press release pointedly highlights that:

---

[1] Sources cited for 7: China Law Translate, PRC National Intelligence Law (as amended in 2018), (March 17, 2021). https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/; 8: Marc A. Thiessen, TikTok, Not Twitter, Is the Real Menace, American Enterprise Institute (December 3, 2022). https://www.aei.org/op-eds/tiktok-not-twitter-is-the-real-menace/; 9: Emily Baker-White, TikTok Spied on Forbes Journalists, Forbes (Dec. 22, 2022), https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance; 10: Ellen Nakashima, Chinese breach data of 4 million federal workers, The Washington Post (June 4, 2015). https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personneloffice/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

- "Temu is not an online marketplace like Amazon or Walmart. It is a data-theft business that sells good online as a means to an end"; and that

- "Though it is known as an e-commerce platform, Temu is functionally malware and spyware. It is purposely designed to gain unrestricted access to a user's phone operating system. It can override data privacy settings on users' devices, and it monetizes this unauthorized collection of data [by selling it to third parties]."

54. Significantly, the Attorney General's complaint memorandum filed in the civil lawsuit highlights that "[e]ven users without the Temu app are subject to Temu's gross overreach if any of their information is on the phone of a Temu user."

55. The complaint memorandum also repeatedly cites the Grizzly Report, in addition to further research and sources corroborating or otherwise supplementing its conclusions.

56. Note as well that there are several Class Actions Complaints that have been filed in the United States advancing substantially similar allegations, including Hu v. Whaleco, Inc., Case 1:23-cv-06962-MKB-PML (U.S. District Court for the Eastern District of New York) and Ziboukh, et al. v. Whaleco Inc. et al., Case 1:23-cv-15653 (U.S. District Court for the Northern District of Illinois). Note that the Hu case was filed on behalf of 13 named plaintiffs from New York, Pennsylvania, Florida, Illinois, Massachusetts, California, Oregon, New Jersey, Georgia, Missouri, Connecticut, Washington, and Texas, and that the Ziboukh case was filed on behalf of 17 named plaintiffs from Illinois, California, Massachusetts, and Virginia, as well as unnamed and others similarly situated.

57. These class actions concern violation of state and federal privacy and consumer protection laws, as well as violations of the US federal Wiretap Act, Electronic Communications Privacy Act, and Computer Fraud and Abuse Act.

Summary of Problematic Practices Giving Rise to the Present Proposed Class Action

58. The Defendants collect, compile, store, and/or disseminate user data exceeding that which is reasonably necessary for online shopping applications such as Temu, deploying a

sophisticated arsenal of covert tools exfiltrating the totality of private data contained on a user's device. In particular, the app's code is intentionally designed to circumvent the Google Play and Apple App Store's respective privacy and security requirements and the front-end security settings on a user's phone by recompiling or changing its own code after being downloaded to a user's phone. At this point, the exfiltration, spying, surveillance, and grossly disproportionate collection, retention, and disclosure of users' personal information and data commences in earnest.

59. The Defendants' intentional and grossly excessive collection of personal user data extends to users' precise geospatial location, and biometric information such as facial characteristics, fingerprints and voiceprints.

60. The Temu application is also used by the Defendants to conduct surreptitious surveillance of app users by bypassing their phones' security systems, enabling the Defendants to track notifications, access and read users' private messages, gain access to the passwords, contacts, calendars, pictures, cameras and microphones on users' phones, make changes to the settings on users' phones, and obtain system information and phone serial (MAC) numbers. Activity on other apps operating on users' devices are also tracked, including in real-time.

61. The Defendants' intentional, excessive, surreptitious, and grossly disproportionate collection of personal information has been and continues to be furthered facilitated, or otherwise advanced by their insufficient disclosure of the nature, level, extent and quantity of data collected through the Temu app to actual and prospective users. The app's design and Temu's data collection, retention and disclosure practices betray the Temu Privacy Policy, which is riddled with misrepresentations, omissions, and withholding of material facts in respect of said practices. Users are thus unable to effectively consent to the Defendants' collection of their data and to ascertain how their personal data and information is used by the Defendants.

62. The Defendants' egregious data collection, retention, surveillance, spying, and exfiltration practices also adversely impact Class Members who are not Temu users and have never downloaded the app or otherwise interacted with it. Such non-user Class Members who have engaged in electronic communications with Temu users such as Plaintiff and user Class Members – including via email, phone, or text messaging – have had their private communications subject to surreptitious surveillance and harvesting by Defendants. Further, non-user Class Members whose information has been stored on the phones and other devices Class Members who have used Temu have also had their personal data and information harvested and/or exfiltrated by the Defendants.

63. The violations of Plaintiff and Class Members' privacy rights are compounded by the exposure of their personal information to misappropriation or compelled disclosure by individuals and entities part of, or affiliated with, the People's Republic of China and/or the Chinese Communist Party.

64. Class Members were entirely unaware of the Defendant's sophisticated surveillance and data exfiltration technologies deployed on the Temu app prior to their public disclosure in the media and investigative reports and were not given any opportunity to consent to them. Any consent provided by Class Members in using the Temu app did not extend to surveillance and the exfiltration, compilation and sharing of their data with third parties, none of which were disclosed to Class Members.

65. As a result of the unauthorised practices mentioned herein, the Plaintiff and Class Members have been deprived by suffering an egregious legally-cognizable and compensable loss and violation of privacy, which also has an economic value to them and to the Defendants.

66. Temu's actions were unconscionable. In circumstances in which the Defendants completely control the operation of the Temu app, and where users have no visibility into its mechanism of action, they took advantage of their position of power over users to exploit them and benefit itself. The Defendants took advantage of the inability of users, including the Plaintiff and Class Members, to protect their own interests because of ignorance or

inability to understand the existence, nature or character of data exfiltration and surveillance practices addresses.

67. Temu's actions breached the Criminal Code, sections 184(1), 184.5, 191(1), 193(1), 402.1 and 402.2(2). These gross violations of privacy negate any justification, which is denied, for the surveillance of Temu users and the exfiltration of their data.

PART 2 – RELIEF SOUGHT

68. An order certifying this action as a class proceeding under the *Class Proceedings Act,* RSBC 1996, c 50;

69. Statutory damages for breaches of s. 1 of the *Privacy Act*, RSBC 1996, c 373 and analogous provincial and territorial legislation;

70. Statutory damages for breaches of s. 5 and/or 8 of the *Business Practices and Consumer Protection Act*, SBC 2004, chapter 2 and analogous provincial and territorial legislation;

71. Damages for the tort of intrusion upon seclusion;

72. Punitive damages;

73. An injunction to restrain the impugned practice by the Defendants;

74. Interest under the *Court Interest Act*, RSBC 1996, c. 79;

75. Such further and other relief as this Honourable Court may deem just.

PART 3 – LEGAL BASIS

76. The Plaintiff pleads and relies on the *Class Proceedings Act*, the *Privacy Act*, and the *Business Practices and Consumer Protection Act*.

Privacy Act

77. The *Privacy Act*, RSBC 1996, c 373, s 1 creates a tort, actionable without proof of damage, where a person, wilfully and without a claim of right, violates the privacy of another.

78. The Defendants acts as set out above constitute "eavesdropping or surveillance" on Class Members within the meaning of the *Privacy Act*, s. 1(4). In particular, the Defendants have been and continue to collect, compile, store, and/or disseminate user data exceeding that which is necessary for online shopping applications such as Temu, deploying a sophisticated arsenal of tools exfiltrating the totality of private data contained on a user's device. The Defendants also conduct surreptitious surveillance of app users by bypassing users' phones' security systems and enabling the Defendants to access and read users' private messages, track notifications, and make changes to the settings on users' phones.

79. Subsection 1(4) is not exhaustive in defining violations of privacy.

80. The Plaintiff and Class Members resident in British Columbia are entitled to statutory damages as a result of the Defendants' breaches under the *Privacy Act*, s. 1.

81. Class Members resident in Manitoba, Newfoundland and Labrador, and Saskatchewan are also entitled to statutory damages, as the *Privacy Act*, CCSM c. P125 (section 2); the *Privacy Act*, RSNL 1990, c. P-22 (section 3), and the *Privacy Act*, RSS 1978, c. P-24 (section 2) respectively also provide for a tort actionable without proof of damage for a person, wilfully, and without claim of right, to violate the privacy of another.

Business Practices and Consumer Protection Act

82. Part 2 of the *Business Practices and Consumer Protection Act*, SBC 2004, chapter 2 prohibits "Deceptive Acts or Practices" (Division 1) and "Unconscionable Acts or Practices" (Division 2). Section 171(1) provides for a right of action for any person who has suffered damage or loss due to the contravention of the Act by a "supplier… who engaged in or acquiesced in the contravention that caused the damage or loss."

83. The Defendants are, individually and collectively, "suppliers" under the Act. Section 1 of the Act defines "supplier" as follows:

> **"supplier"** means a person, whether in British Columbia or not, who in the course of business participates in a consumer transaction by
>
> (a) supplying goods or services or real property to a consumer, or
>
> (b) soliciting, offering, advertising or promoting with respect to a transaction referred to in paragraph (a) of the definition of "consumer transaction",
>
> whether or not privity of contract exists between that person and the consumer, and includes the successor to, and assignee of, any rights or obligations that person… (emphasis added throughout)

84. Paragraph (a) of the definition of "consumer transaction" reads as follows: "(a) a supply of goods or services or real property by a supplier to a consumer for purposes that are primarily personal, family or household".

85. In essence, each Defendant individually and collectively as each other's agents and alter egos "participates in a consumer transaction" by "soliciting, offering, advertising or promoting" the "supply of goods" to Temu users on behalf of, in association with and/or for the benefit of, the merchants and sellers and other entities who are themselves "suppliers" and supply goods to Temu users who purchase the goods by way of the Temu app.

86. This is so even if one assumes that "no privity of contract exists" between Temu and Temu users – which is not at all conceded by the Plaintiff and Class Members. As the definition

also makes clear, the Act applies to PDD Holdings and Whaleco Inc. as it applies to a person "whether in British Columbia or not".

87. The Defendants have individually and collectively violated the Act by engaging in or acquiescing in Unfair Practices identified in Part 2 thereof – namely, Deceptive Acts or Practices identified in Division 1 and/or Unconscionable Acts or Practices listed in Division 2.

88. Section 4(1) of the Act defines "deceptive act or practice" to "mean[], in relation to a consumer transaction,":

> (a) an oral, written, visual, descriptive or other representation by a supplier, or
>
> (b) any conduct by a supplier
>
> that has the capability, tendency or effect of deceiving or misleading a consumer...

89. In turn, the term "representation" is non-exhaustively defined in s. 4(1) to "include[] any term or form of a contract, notice or other document used or relied on by a supplier in connection with a consumer transaction" and s. 4(2) specifies that "[a] deceptive act or practice by a supplier may occur before, during or after the consumer transaction."

90. The non-exhaustive list of representations enumerated in s. 4(3) and prohibited under s. 5(1) as Unfair Acts or Practices includes the following:

> (a) a representation by a supplier that goods or services
>
> [...]
>
> (iv) are available for a reason that differs from the fact
>
> [...]

(b) a representation by a supplier

[…]

(iii) that the purpose or intent of a solicitation of, or a communication with, a consumer by a supplier is for a purpose or intent that differs from the fact,

(iv) that a consumer transaction involves or does not involve rights, remedies or obligations that differs from the fact,

(v) that uses exaggeration, innuendo or ambiguity about a material fact or that fails to state a material fact, if the effect is misleading (emphasis added)

91. Section 9(1) prohibits committing or engaging in "an unconscionable act or practice in respect of a consumer transaction." Section 8(1) specifies that such "act or practice by a supplier may occur before, during, or after the consumer transaction." Importantly, the definition of "unconscionable acts or practices" is not exhaustive but instead involves a contextual assessment in which "a court must consider all of the surrounding circumstances of which the supplier knew or ought to have known" (s. 8(2)), which include, but are not limited to the non-exhaustive circumstances listed in s. 8(3). The listed circumstances most pertinent to the present proposed class proceeding are

[…]

(c) that the supplier took advantage of the consumer or guarantor's inability or incapacity to reasonably protect the consumer or guarantor's own interest because of physical or mental infirmity, ignorance, illiteracy, age or inability to understand the character, nature, or language of the consumer transaction, or any other matter related to the transaction;

[…]

(e) that the terms or conditions on, or subject to, which the consumer entered into the consumer transaction were so harsh or adverse to the consumer as to be inequitable;

92. The Defendants have individually and collectively violated the Act by engaging in or acquiescing in Unfair Practices identified in Part 2 thereof – namely, Deceptive Acts or Practices identified in Division 1 and/or Unconscionable Acts or Practices listed in Division 2 – by using the inducement of cheaply-priced Chinese-made goods to entice the

Plaintiff and Class Members to download, make purchases and continue using the Temu app in order to unknowingly and unwittingly provide near-limitless access to their sensitive personal data and information.

93. The Defendants' intentional withholding, misrepresentations and/or omissions of key information pertaining to their data collection, retention, and disclosure practices -- as well the misleading effects of said practices – constitute the core of their Deceptive and/or Unconscionable Acts or Practices.

94. Note that s. 5(2) involves a reversal of the burden of proof on the supplier: "If it is alleged that a supplier committed or engaged in a deceptive act or practice, the burden of proof that the deceptive act or practice was not committed or engaged in is on the supplier." As a result, it falls upon the Defendants to individually and collectively establish on a balance of probabilities that they did not engage in Deceptive Acts and/or Practices.

95. The Defendants' privacy-violative deceptive and/or unconscionable acts and/or practices are executed through code and are therefore invisible to average laypersons renders said acts and practices even more egregious, as there is no way for Plaintiff and Class Members could have known the full extent of the nature of the privacy harms visited upon them by the app. Indeed, Defendants' conduct is especially egregious in light of the lengths to which they go to prevent independent third parties—including security researchers, Google, and Apple—from uncovering their bad acts.

96. A reversal of the burden of proof also operates under s. 9(2): "If it is alleged that a supplier committed or engaged in an unconscionable act or practice, the burden of proof that the unconscionable act or practice was not committed or engaged in is on the supplier."

97. The Plaintiff and Class Members respectively and collectively suffered legally cognizable and compensable damages and/or losses due to the Defendants engaging in or acquiescing in the Unfair and/or Unconscionable Acts or Practices that caused said damages and/or

losses. Damages or losses arising from the Defendants' contraventions of the Act are therefore recoverable under s. 171(1).

98. Class Members situated in provinces and territories other than British Columbia rely on analogous provisions in provincial and territorial consumer protection and/or business practices legislation.

Tort of Intrusion Upon Seclusion

99. The Defendants committed the tort of intrusion upon seclusion, a common law tort actionable without proof of harm and that is crystallized when a defendant:

    a. intentionally or recklessly;

    b. invades a plaintiff's private affairs or concerns;

    c. without lawful justification;

    d. where a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

100. The Defendants committed the tort of intrusion upon seclusion by collecting, compiling, storing, and/or disseminating user data exceeding that which is necessary for online shopping applications such as Temu, deploying a sophisticated arsenal of tools exfiltrating the totality of private data contained on a user's device. The Defendants also conduct surreptitious surveillance of app users by bypassing users' phones' security systems and enabling the Defendants to access and read users' private messages, track notifications, and make changes to the settings on users' phones.

101. The Defendants intentionally, or at a minimum recklessly, invaded the private affairs or concerns of the Class Members. The Defendants' actions were without lawful justification. A reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

102. Class Members are entitled to damages as a result of the Defendants' tortious acts.

Punitive Damages

103. The Defendants' misconduct as described above, was malicious, oppressive and highhanded, and markedly departed from ordinary standards of decent behaviour. The Defendants repeatedly and egregiously violated the trust and security of Class Members.

104. The Defendants did it deliberately, knowing that they did not obtain Class Members' consent and deliberately attempted to conceal their wrongdoing. The Defendants' actions offend the moral standards of the community and warrant this Honourable Court's condemnation. An award of punitive damages should therefore be ordered.

Joint and Several Liability

105. The Defendants are jointly and severally liable for the acts of each of them.

Injunction

106. The Plaintiff and Class Members are entitled to an injunction under the *Law and Equity Act*, RSBC 1996, c 253 to restrain this conduct by the Defendants now and into the future.

Discoverability

107. The Plaintiff and Class Members could not reasonably have known that:

a. they sustained injury, loss or damage as a consequence of the Defendants' actions; or

b. having regard to the nature of their injuries, losses or damages, a court proceeding would be an appropriate means to seek to remedy the injuries, losses or damages until, at the earliest, on April 3, 2023 when CNN broke the story.

108. The Plaintiff and Class Members plead and rely on postponement and discoverability under the *Limitation Act*, SBC 2012, c 13, s. 8.

109. In addition, the Defendants, willfully concealed the exfiltration and misuse of the Plaintiff and Class Members' personal information and surveillance of their phones without consent, and that this was caused or contributed to by the Defendants' acts or omissions. The Plaintiff and Class Members rely on *Pioneer Corp. v. Godfrey*, 2019 SCC 42 and the *Limitation Act*, s 21(3).

Service on Out-of-Province Defendants

110. The Plaintiff and Class Members have the right to serve this Notice of Civil Claim on the Defendants pursuant to the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28, s 10 (CJPTA), because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based.

a. a tort committed in British Columbia (CJPTA, s. 10(g)); and
b. a business carried on in British Columbia (CJPTA, s. 10(h)).

111. An action under the Privacy Act must be determined in the Supreme Court of British Columbia (*Privacy Act*, s. 4).

Plaintiff's address for service:

Consumer Law Group P.C.
150 Elgin Street, 10th Floor
Ottawa, ON K2P 1L4

Fax number for service: (613) 627-4893

Email address for service:
jorenstein@clg.org
ldavid@clg.org

The address of the registry is:

800 Smithe Street
Vancouver, BC
V6Z 2E1
Place of Trial Vancouver
Date: October 1, 2024

Signature of lawyer for plaintiff
Jeff Orenstein
LSO # 59631G

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

(1) 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

The plaintiff claims the right to serve this pleading on the Defendants Whaleco Inc. and PDD Holdings Inc. outside British Columbia on the ground that the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c. 28, s. 10 (*CJPTA*) applies because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based. The Plaintiff and Class Members rely on the following grounds, in that this action concerns:

a. a tort committed in British Columbia (*CJPTA*, s. 10(g)); and
b. a business carried on in British Columbia (*CJPTA*, s. 10(h)).

Appendix

[*The following information is provided for data collection purposes only and is of no legal effect.*]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a claim for damages arising out of Temu's breaches of privacy through unauthorised collection of user data and unfair and/or unconscionable acts and/or practices.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident
[ ] medical malpractice
[x] another cause

A dispute concerning:

[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] personal property
[x] 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:

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

Part 4:

Business Practices and Consumer Protection Act, SBC 2004, chapter 2
Court Jurisdiction and Proceedings Transfer Act, SBC 2003, c 28
Court Order Interest Act, RSBC 1996, c 79
Privacy Act, RSBC 1996, c 373