Court File No. CV-16-566248-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N

NATALIA KARASIK

Plaintiff

and

YAHOO! INC. and YAHOO! CANADA CO.

Defendants

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

Notice of Action issued on December 16, 2016

I. RELIEF SOUGHT

1. The plaintiff, on her own behalf and on behalf of the Class Members (as defined below), claims:

(a) an order pursuant to the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 (the "*CPA*"), certifying this action as a class proceeding and appointing her as representative plaintiff of the Class;

(b) a declaration that the defendants owed a duty of care to the plaintiff and the Class Members, and breached the standard of care owed to them;

(c) a declaration that the defendants breached the Contracts (as defined below);

(d) a declaration that the defendants breached section 219 of the *Consumer Protection Act*, C.Q.L.R., c. P-40.1 (the "*Consumer Protection Act*"), with regard to Class Members resident in Quebec;

(e) a declaration that the defendants breached the confidence of the plaintiff and the Class Members;

(f) a declaration that the defendants intruded upon the seclusion of the plaintiff and the Class Members;

(g) a declaration that the defendants committed the tort of publicity given to private life;

(h) a declaration that the defendants were unjustly enriched, to the deprivation of the plaintiff and the Class Members;

(i) damages in the amount of $50 million dollars;

(j) punitive damages in the amount of $10 million dollars jointly and severally as against all defendants;

(k) an order, pursuant to s. 24 of the *CPA*, directing an aggregate assessment of damages;

(l) an order directing a reference or giving such other directions as may be necessary to determine any issues not determined at the trial of the common issues;

(m) pre-judgment and post-judgment interest, compounded, or pursuant to ss. 128 and 129 of the *Courts of Justice Act*, R.S.O. 1980, c. 43 (the "*CJA*");

(n) costs of this action on a partial indemnity basis, together with applicable HST or other applicable taxes thereon;

(o) the costs of administering the plan of distribution of the recovery in this action; and

(p) such further and other relief as this Honourable Court deems just.

II. OVERVIEW

2. On September 22, 2016, Yahoo! Inc. ("**Yahoo**") sent a mass email to some of its users, informing them that a recent internal investigation had confirmed that their account information had been stolen from Yahoo's network in a cyberattack in late 2014 (the "**2014 Breach**"). The stolen user account information included names, email addresses, telephone numbers, dates of birth, hashed passwords, and both encrypted and unencrypted security questions and passwords.

3. In a press release distributed that same day, Yahoo confirmed that information from at least 500 million user accounts was included in the 2014 Breach.

4. On December 14, 2016, Yahoo sent another mass email to some of its users, informing them that there had been a distinct, earlier cyberattack on Yahoo's network in August 2013 (the "**2013 Breach**"). The stolen user account information in the 2013 Breach also included names, email addresses, telephone numbers, dates of birth, hashed passwords, and both encrypted and unencrypted security questions and passwords.

5. In a press release distributed that same day, Yahoo confirmed that information from over one billion user accounts was included in the 2013 Breach.

6. Yahoo confirmed in documents it filed with the United States Securities and Exchange Commission on November 9, 2016 that Yahoo had knowledge of the 2014 Breach in 2014 shortly after it had occurred.

7. User account information stolen in the 2013 and 2014 Breaches was made available for sale on the "dark web" (an encrypted internet network which requires specific software to

access) in the years between when the Breaches occurred, and when Yahoo publicly announced that they had taken place.

8. It is highly likely that Yahoo user accounts (the "Yahoo Accounts") were accessed given the breadth of account information that was leaked, and given Yahoo's practice of hashing passwords with the relatively weak MD5 algorithm.

9. Yahoo's press release on December 14, 2016 further indicated that hackers propagated forged cookie files in separate attacks through 2015 and 2016, which provided another avenue for intruders to access Yahoo user accounts which was most probably utilized.

III. CLASS DEFINITION

10. The plaintiff brings this action on behalf of all persons residing in Canada whose Yahoo account information was stolen in the 2013 Breach, the 2014 Breach and/or through the use of forged cookies in 2015 and/or 2016, excluding the defendants and the defendants' executives (the "**Class**" or "**Class Members**").

IV. THE PARTIES

A. Plaintiff

11. The plaintiff Natalia Karasik ("**Natalia**") is an individual who resides in Barrie, Ontario. She has used a *Yahoo! Mail* account as her primary personal email service for over ten years. Natalia received Yahoo's press release on December 14, 2016 which stated, among other things, that Yahoo "believe an unauthorized third party, in August 2013, stole data associated with a broader set of user accounts, including [hers]."

B. Defendants

12. The defendant, Yahoo! Inc. (previously defined as "Yahoo") is a publically-traded technology company, incorporated pursuant to the laws of Delaware and headquartered in Sunnyvale, California, U.S.A. Yahoo operates numerous online services including the following:

(a) *Yahoo! Mail* ("*Mail*"), a web-based email service;

(b) *Yahoo! Messenger* ("*Messenger*"), an instant messaging service;

(c) *Yahoo! Search ("Search*"), a search engine;

(d) *Yahoo! Groups* ("*Groups*"), a provider of online discussion boards;

(e) *Yahoo! News* ("*News*"), an online news aggregator;

(f) *Yahoo! Finance* ("*Finance*"), a financial data provider with personal finance management tools;

(g) *Flickr*, and image and video hosting service; and

(h) *Tumblr*, a blogging and social networking website.

13. Yahoo was a pioneering internet firm in the 1990s and continues to offer some of the most popular websites on the internet. At the time of pleading, Yahoo has a market capitalization of over $4 billion on the NASDAQ Stock Exchange. The company's 2014 Annual Report indicates that they had "more than 1 billion monthly active users" and the 2015 Annual Report indicates they have more than 600 million monthly mobile users as of December 31, 2015.

14. The defendant, Yahoo! Canada Co. ("**Yahoo Canada**") was at all material times a subsidiary of Yahoo, incorporated pursuant to the laws of Nova Scotia and headquartered in Toronto, Canada. Yahoo Canada operates versions of certain Yahoo services geared towards a Canadian audience, including *Mail*, *News* and *Finance*.

15. Yahoo provides services to Canadians in conjunction with Rogers Communications Inc. This enterprise is described on the website located at ca.rogers.yahoo.com as "*Rogers Yahoo*" and *"Rogers powered by Yahoo*". Some of the services on offer are described on the same website as "*Rogers Yahoo! Homepage*", "*Rogers Yahoo! Mail*" and "*Rogers Yahoo! Search*". The login page to the these services includes an "Account Security Notice" along with a link to Yahoo's September and December Security Notices, which are further particularized below.

V. FACTS SUPPORTING THE PLAINTIFFS' CLAIMS AGAINST THE DEFENDANTS

A. Background

1. What is Account Information?

16. The defendants offer the above-noted and other services openly to all members of the public. In order to access these services, one must first create a Yahoo Account by providing a username and associated password which is thereafter used to login to Yahoo services, along with a security question and answer (such as the user's mother's maiden name) that can be used to generate a new password in the event that the original password is lost. At the time of account creation, and periodically thereafter, the defendants request certain identifying information consisting of first name, last name, mobile telephone number, date of birth and gender. Collectively, the username, password, security question and answer, and identifying information, will be hereinafter referred to as the "**Account Information**". It constitutes the information required to login to a Yahoo account, either by entering the username and password or, alternatively, by generating a new password with the security question and answer.

2. Account information is highly sensitive

17. Account Information is highly sensitive because it is the information people use to access their own accounts. If a third-party obtains a user's sufficient Account Information, the third-party will be able to access the user's account repeatedly and at will, as if the account belonged to the third-party. The user may never know that a third-party is accessing the user's accounts.

3. Account Information provides access to multiple Yahoo services

18. One Yahoo Account can be associated with multiple Yahoo services. For example, a user may send and receive emails with *Mail*, track his/her investments with *Finance*, and share his/her photos on *Flickr*. The same username and password could be used to login to all three services. In many cases, logging-in to one service will cause the user to be automatically logged-in to the other services. As a result, a third-party who obtains that user's sufficient Account Information will be able to access a wider breadth of private information stored across multiple Yahoo services.

4. Yahoo Accounts are highly sensitive

19. When a third-party obtains a user's Account Information and is able to access an associated Yahoo Account, a significant invasion of privacy may result because a Yahoo Account can contain highly sensitive information across all facets of a person's life. For example, a Yahoo email account may contain: personal health information disclosed in correspondence with healthcare providers and insurers; personal financial information disclosed in bank and credit card statements, tax returns, and communications with financial professionals; and all sorts of political, religious and otherwise personal opinions and beliefs disclosed in private communications with friends and family.

5. Access to email provides access to non-Yahoo services

20. If a third-party is able to access a Yahoo user's email account, the third-party will usually be able to access additional services offered by companies other than Yahoo. This is because most online services with a user login will provide a method for retrieving the username or password in the event that the user loses either or both. The most common method of retrieval is to email to the user a link to a website where the user (or anyone with access to the user's email) may generate a new password for the online service. In this way, access to an email address may provide access to that user's online banking portal, Canada Revenue Agency portal, and to a host of other sensitive personal information.

6. Disclosure of Account Information renders a user's non-Yahoo accounts vulnerable

21. Internet users frequently recycle usernames passwords across multiple accounts. Thus, disclosure of a Yahoo-associated Account Information may allow third-parties to access non-Yahoo-related accounts by simply entering the same Account Information.

7. Disclosure of Account Information exposes users to phishing and other scams

22. Parties who engage in online scams will use lists of email addresses disclosed in data breaches to send mass emails in an attempt to obtain sensitive information – such as account information or banking information – by posing as a trustworthy source, in a practice called "phishing". Thus, disclosure of an email address renders a person more likely to be targeted for online scams, and ultimately more likely to fall victim to a phishing or other scam.

8. The defendants were responsible for protecting the Account Information

23. The defendants stored the Account Information electronically on data servers. They were and continue to be responsible for safeguarding the Account Information. To the extent that

either defendant delegated to the other, and/or to any other party or parties, responsibility for collecting, managing, storing, securing and/or deleting Account Information, the delegating defendant is directly liable for resultant damages because both defendants hold a non-delegable duty to secure Account Information.

B. Yahoo's privacy standards

24. Yahoo has a Privacy Policy which states as follows:

> **Information Collection and Use**
>
> **General**
>
> When you register we ask for information such as your name, gender, birth date, postal code and email address. Once you register with Yahoo and sign in to our services, you are not anonymous to us.
>
> …
>
> **Confidentiality and Security**
>
> We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.
>
> We have physical, electronic, and procedural safeguards that comply with our legal obligations to protect personal information about you.
>
> To learn more about security, including the security steps we have taken and security steps you can take, please read Security at Yahoo.

25. The Security at Yahoo document referenced in the Privacy Policy states as follows:

> Protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust.
>
> …
>
> **Secure Storage**
>
> We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.

26. Yahoo's website Terms of Condition and Use state:

> **YAHOO PRIVACY POLICY**

> Registration Data and certain other information about you is subject to our Privacy Policy. For more information, see our full privacy policy at http://privacy.yahoo.com/privacy/ca/. You understand that through your use of the Service you consent to the collection, use and disclosure of this information, only as permitted by the Privacy Policy, including the transfer of this information to the United States and/or other countries for storage, processing, and use by Yahoo and its affiliates in order to provide the Service to you.
>
> The Yahoo I.D. associated with your account is the property of Yahoo or its affiliates, and is not your personal information.
>
> **MEMBER ACCOUNT, PASSWORD, AND SECURITY**
>
> During registration for a Yahoo I.D., you will select a password and Yahoo I.D. Upon successful registration for the Service, you will receive an account designation. You understand and agree that you are solely responsible for maintaining the confidentiality of your account including your password, and are fully responsible for all activities that occur under your account, including your password. You agree to (a) immediately notify Yahoo of any unauthorized use of your password or account or any other breach of security, and (b) exit from your account at the end of each session. Yahoo will not be liable for any loss or damage arising from your failure to comply with this Section 5.
>
> …
>
> **General Information**
>
> Choice of Law and Forum. The TOS and the relationship between you and Yahoo shall be governed by the laws of the province of Ontario and Canada without regard to its conflict of law provisions. You and Yahoo agree to submit to the personal and exclusive jurisdiction of the courts located within the province of Ontario, Canada.

C. The 2014 Breach

27. On September 22, 2016, Yahoo published a Security Notice on Yahoo.com ("**September Security Notice**") and emailed the same to its account holders, advising that in late 2014 a third-party, "state-sponsored" intruder stole "a copy of certain user account information" including "names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers." Yahoo officials later indicated that 500 million accounts were affected.

28. The September Security Notice indicated that Yahoo is investigating the attack with "law enforcement authorities", and that the investigation "has found no evidence that the state-sponsored actor is currently in Yahoo's network."

29. The September Notice also explained the concept of a "hashed password" and the computer algorithm Yahoo used to performing the hashing:

> **What is a "hashed password"?**
>
> Hashing is a oneway mathematical function that converts an original string of data into a seemingly random string of characters. As such, passwords that have been hashed can't be converted into the original plain text password.
>
> **What is "bcrypt"?**
>
> Bcrypt is a password hashing mechanism that incorporates security features, including salting and multiple rounds of computation, to provide advanced protection against password cracking.

The concept of hashing passwords is further particularized below.

D. The 2013 Breach

30. On December 14, 2016, Yahoo published a Security Notice on Yahoo.com ("**December Security Notice**") and emailed the same to Yahoo account holders, including the plaintiff, advising that an unauthorized third-party had stolen Account Information of 1 billion users in August 2013. The leaked Account Information was said to include "names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers."

31. Yahoo indicated that this breach came to their attention after law enforcement provided Yahoo with data files in November 2016, and that Yahoo "believe[d] that the August 2013 incident is likely distinct from the incident [they] disclosed on September 22, 2016."

32. Yahoo claimed to have "invalidated unencrypted security questions and answers so that they cannot be used to access an account," but did not provide a timeframe for when this measure was taken.

33. The December Security Notice advised of a separate incident in 2015 and 2016 involving "the creation of forged cookies that could allow an intruder to access users' accounts without a password." The December Security Notice explained the concept of "cookies" as follows:

> **What is a "cookie"?**
>
> A cookie is a small piece of information stored on a computer for the purpose of identifying a web browser during interaction on websites. Websites use cookies to remember and recognize details about visitors, such as website preferences.

34. The December Security Notice further advised users to " to remain vigilant by reviewing your account statements and monitoring your credit reports", provided the contact details for three credit reporting agencies, and suggested users purchase fraud alert or security freezing services from the credit agencies.

E. Yahoo's discovery of the Breach

35. Yahoo confirmed in a Quarterly Report it filed with the United States Securities and Exchange Commission on November 9, 2016 that Yahoo had knowledge of the 2014 Breach in 2014 shortly after it had occurred. The Quarterly Report provides the following:

> In late July 2016, a hacker claimed to have obtained certain Yahoo user data. After investigating this claim with the assistance of an outside forensic expert, the Company could not substantiate the hacker's claim. Following this investigation, the Company intensified an ongoing broader review of the Company's network and data security, including a review of prior access to the Company's network by a state-sponsored actor that the Company had identified in late 2014. Based on further investigation with an outside forensic expert, the Company disclosed the Security Incident on September 22, 2016, and began notifying potentially affected users, regulators, and other stakeholders.

> The Company, with the assistance of outside forensic experts, continues to investigate the Security Incident and related matters. The Company is actively working with U.S. law enforcement authorities on this matter.
>
> As described above, the Company had identified that a state-sponsored actor had access to the Company's network in late 2014. An Independent Committee of the Board, advised by independent counsel and a forensic expert, is investigating, among other things, the scope of knowledge within the Company in 2014 and thereafter regarding this access, the Security Incident, the extent to which certain users' account information had been accessed, the Company's security measures, and related incidents and issues.
>
> In addition, the forensic experts are currently investigating certain evidence and activity that indicates an intruder, believed to be the same state-sponsored actor responsible for the Security Incident, created cookies that could have enabled such intruder to bypass the need for a password to access certain users' accounts or account information.
>
> Separately, on November 7, 2016, law enforcement authorities began sharing certain data that they indicated was provided by a hacker who claimed the information was Yahoo user account data. Yahoo will, with the assistance of its forensic experts, analyze and investigate the hacker's claim that the data is Yahoo user account data. [emphasis added]

F. The release of the information

36. Yahoo Account Information has been reportedly sold on online black markets located on the dark web, which is an encrypted internet network which requires specific software and to access. Account Information from the 2013 Breach was reportedly sold to three buyers for $300,000 in August 2015.

G. Yahoo's inadequate cyber security measures/safeguards

37. Yahoo failed to fortify its systems against adverse intruders. Yahoo further failed to sufficiently encrypt and hash Account Information in the event that it was obtained by third-parties.

1. Hashed passwords

38. Online services do not typically store user passwords as plaintext because any party who obtains that information would be able to immediately access the users' accounts. One alternative to storing passwords as plaintext is to store a "hash digest" of passwords.

39. The process is generally as follows. At the time of account creation, a user's password is processed through a complicated mathematical algorithm called a "cryptographic hash function", and the resultant answer or "hashed password" is a long string of characters which is stored on the online service's computer systems along with the cryptographic hash function. When the user wishes to thereafter login by entering his or her password, the password is again processed through the same cryptographic hash function producing a second hashed password. The two hashed passwords are then compared and, if they match, the user will be "authenticated" and able to login. The collection of hashed passwords saved on a system is called the "hash digest".

40. Hashing is secure means of managing passwords when it is a one-way process, meaning the hashed password is created by processing the plaintext password through the cryptographic hash function, but the plaintext password cannot be reconstructed from the hashed password and the cryptographic hash function.

41. Yahoo's September Security Notice advised that the "vast majority" of passwords leaked in the 2014 Breach were hashed with the bcrypt algorithm, which may or may not provide adequate protection. However Yahoo's December Security Notice included "hashed passwords (using MD5)" in the list of leaked Account Information. MD5 refers to is an obsolete hashing algorithm that suffers from extensive vulnerabilities and can be reversed, meaning plaintext passwords can be reconstructed from the hashed passwords that Yahoo has admitted were stolen.

42. Once a third-party reconstructs a Yahoo users' password, the third-party would be able to access the Yahoo account at will as if it belonged to the third-party. Given the quantity of leaked

Account Information, and given Yahoo's use of the weak MD5 algorithm, it is probable that Class Members' accounts have been accessed by third-parties. The Class Members would likely have no knowledge of this intrusion.

2. Unencrypted security questions and answers

43. Both the September and December Security Notices indicated that "encrypted or unencrypted security questions and answers" had been leaked. As indicated above, a security question and answer is provided at the time of account creation and is used to retrieve a lost username or password. One common example is to provide the user's mother's maiden name.

44. A third-party who obtains a user's unencrypted security question and answer may be able to access a user's account as if the third-party had the username and password. The user would likely have no knowledge of this intrusion. Given the quantity of leaked Account Information, and given the ease with which a third-party may access an account with unencrypted security questions and answers, it is probable that Class Members' accounts have been accessed by third-parties. The Class Members would likely have no knowledge of this intrusion.

45. The risks associated with a third-party obtaining a user's encrypted security question and answer will depend on the kind and quality of encryption. Yahoo's Security Notices do not indicate the method of encryption used.

3. Use of forged cookies

46. Yahoo's December Security Notice indicated that forged cookies had been propagated and may provide a third-party access to Yahoo user accounts. Authentication cookies are text files that contain information about the user's previous sessions with Yahoo, including whether the user has already been authenticated and logged-in to Yahoo's servers. A forged cookie may bypass the authentication login process and grant a third-party access to the user's Yahoo

Account without needing to supply the username and password. Such unauthorized access may continue for any duration. Given the number of Canadians using Yahoo services, it is probable that Class Members' accounts were accessed by third-parties with the use of forged cookies. The Class Members would likely have no knowledge of this intrusion.

H. Role of Yahoo in Canada

47. The plaintiff brings claims directly against Yahoo because the September and December Security Notices were published by Yahoo and those documents indicate that Yahoo was responsible for securing the Account Information for all users, including Canadian users. Furthermore, Yahoo accounts held by Canadian users are governed by Yahoo's Privacy Policy, which is published by Yahoo, makes no reference to Yahoo Canada, and refers all questions about the Privacy Policy to Yahoo's Privacy Officer based at Yahoo's headquarters in Sunnyvale, California.

VI. CAUSES OF ACTION

A. Negligence

48. The defendants owed a duty of care to the Class Members in their collection and storage of the Account Information, to keep the Account Information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons. Specifically, the defendants owed a duty of care to the Class Members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and to limit the exposure of the Class Members' Account Information even in case of a successful cyberattack.

49. There was a sufficient degree of proximity between the Class Members and the defendants to establish a duty of care because:

a) it was reasonable for the plaintiff and other Class Members to expect that Yahoo, as a major international technology company, had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their Account Information in case of a cyberattack;

b) it was reasonably foreseeable to the defendants that, if a cyberattack resulted in the theft of the Class Members' Account Information, the information in the Class Members' Yahoo Accounts would become vulnerable to theft and the Class Members would sustain damages, such that the defendants should have been mindful of the Class Members' privacy and on guard against a cyberattack;

c) it was reasonably foreseeable to the defendants that, if they failed to take appropriate security measures, there was a risk that the Class Members' privacy would be breached, because of the broad range of sensitive, private data potentially stored in the Class Members' Yahoo Accounts, and the climate of increasing cyberattacks targeted toward technology companies like Yahoo;

d) the Class Members were entirely vulnerable to the defendants, in terms of relying on the defendants to take appropriate security measures to protect their Account Information;

e) the defendants, through the Yahoo Privacy Policy, promised to take appropriate measures to protect the Class Members' Account Information;

f) there is a sufficient degree of proximity between the Class Members and the defendants because the Class Members are, or were, users of Yahoo services;

g) the defendants were required by sections 4.1, 4.5 and 4.7 of Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

(the "*PIPEDA*"), to implement safeguards appropriate to the extreme sensitivity of the Class Members' Account Information;

h) with regard to the Class Members resident in Quebec, the defendants were required by sections 5 and 6 of *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c.P-39.1 ("*PIPPS*") to comply with statutory obligations regarding the collection, retention and disclosure of the Class Members' Account Information;

i) there was a contractual relationship between the Class Members and the defendants.

50. The defendants failed in their duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, securing and/or deleting the Class Members' Account Information, particulars being described in paragraphs 27 to 46 of the claim, above, and further described below:

a) they failed to handle the collection, retention, and security of the Class Members' Account Information in accordance with Yahoo's Privacy Policy;

b) they failed to designate individuals who are responsible and accountable for Yahoo's network security management, including compliance with its internal policies and reasonable industry standards in its collection, storage, protection and destruction of Account Information, as particularized at paragraphs 27 to 46, and contrary to s. 4.1 of Schedule 1 to the *PIPEDA*;

c) they allowed the Account Information to be used and disclosed for purposes other than those for which it was collected, as particularized in paragraphs 27 to 46, and contrary to s. 4.5 of Schedule 1 to the *PIPEDA*;

d) they failed to implement appropriate organizational and technological safeguards to protect the Account Information against loss, theft, unauthorized access, disclosure, copying, use, and/or modification, as particularized in paragraphs 27 to 46, and contrary to s. 4.7 of Schedule 1 to the *PIPEDA*;

e) they failed to comply with the statutory obligations set out in sections 5 and 6 of *PIPPS*;

f) they failed to keep the Class Members' Account Information secure and confidential;

g) they stored the Class Members' Account Information on an insecure network;

h) they failed to encrypt the Class Members' Account Information in accordance with reasonable industry standards;

i) they failed to use any, or appropriate, cybersecurity measures, programs and policies to safeguard the Class Members' Account Information, or they used cybersecurity measures, programs and policies which were outdated, inadequate, and below the reasonable industry standards;

j) they failed to protect the Class Members' Account Information from compromise, disclosure, loss or theft;

k) they failed to take steps to prevent the Class Members' Account Information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet;

l) breaches of contract as particularized below;

m) they failed to hire competent employees, they failed to properly supervise their employees, or they failed to provide proper training to their employees;

n) they failed to inspect their servers at all or to inspect them regularly, in a timely and thorough manner, for potential privacy breaches; and

o) they failed to notify the Class Members of the breach in a reasonably timely manner, and their notice to the Class Members failed to provide sufficient information to allow the Class Members to understand the significance of the breach to them.

51. As a result of the defendants' negligence, anonymous hackers were able to gain access to the Class Members' Account Information, as well as the information in the Class Members' Yahoo Accounts, and to go undiscovered for years resulting in the Class Members sustaining damages.

52. The plaintiff pleads and relies on the *Negligence Act*, R.S.O. 1990, c. N.1 and comparable legislation across Canada.

B. Breach of contract/warranty

53. The plaintiff and every Class Member entered into a contract with Yahoo by filling out a registration form to create a Yahoo Account. In exchange for agreeing that Yahoo could collect, use and store the Class Members' Account Information, customers were granted access to Yahoo Accounts and services. It was an express or implied term of the contract that Yahoo would be responsible for all of the Class Members' Account Information under its control/possession and would utilize appropriate security safeguards to protect the Account Information from unauthorized access and distribution.

54. The Terms and Conditions of Use on all Yahoo websites provide that all of the Account Information, as well as "certain other information" collected by Yahoo, are subject to the Yahoo Privacy Policy. All of the provisions in the Yahoo Privacy Policy, as described above, are

therefore incorporated into the Contracts by virtue of Yahoo's Terms and Conditions of Use. All such terms and conditions have been breached by Yahoo for the reasons described in this claim.

55. Specifically, Yahoo had an express or implied contractual obligation to make reasonable efforts to maintain confidentiality over the Account Information it collected from the plaintiff and the other Class Members and which it stored on its internal computer network, to secure aforesaid Account Information against such risks as unauthorized access, collection, use, disclosure and copying, to regularly monitor its servers to identify any unauthorized access which had taken place, and to permanently delete and destroy outdated customer Account Information, in accordance with its own privacy policies, applicable laws and industry standards. Yahoo breached its Contracts with the Class Members by failing to make such reasonable efforts, as set out in paragraphs 27 to 46, resulting in unauthorized access.

56. Yahoo warranted to the plaintiff and the other Class Members, through its Privacy Policy, that it was committed to protecting their privacy. Yahoo breached its warranty by failing to take reasonable efforts to protect the Class Members' Account Information, as set out in paragraphs 27 to 46, resulting in unauthorized access.

57. Yahoo had an express or implied contractual obligation to comply with applicable privacy legislation and to manage Account Information in a manner that was consistent with the principles that are reflected in such legislation. By promising to comply with applicable privacy legislation in its Privacy Policy, Yahoo also incorporated the legislation into the contract and has breached its contract with the plaintiff and the Class Members by failing to comply with the applicable privacy legislation including *PIPEDA*, as particularized above.

58. With regard to the Class Members resident in Quebec, Yahoo breached its contracts with those Class Members by failing to comply with the applicable privacy legislation including *PIPPS*, as particularized above.

C. Breach of the contractual duties of honesty, and good faith and fair dealing

59. Yahoo had a duty in the performance of its contractual obligations to act honestly and in good faith. At minimum, Yahoo was required to make reasonable efforts to maintain confidentiality over the Account Information it collected from the plaintiff and the other Class Members and stored on its internal computer network, to secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated information.

60. Yahoo promised on its website that it had established reasonable security safeguards for the Class Members' Account Information. Yahoo knew that the Account Information provided by Class Members was highly sensitive in nature, and that the information contained in the Class Members' Yahoo Accounts would also likely be highly sensitive in nature, that the Class Members were unable to assess the cybersecurity measures taken by the defendants, and that the Class Members relied on the defendants to secure their Yahoo Accounts and their Account Information.

61. Yahoo's failure to take reasonable measures to secure the information stored on its network, when it promised and made assurances on its website that it had done so, is a breach of the defendants' duties of honesty, and good faith and fair dealing.

D. Breach of the *Consumer Protection Act*

62. With respect to Class Members resident in Quebec, the defendants are subject to the obligations of the *Consumer Protection Act*, which prohibits persons who enter into agreements

or conduct transactions with consumers from engaging in prohibited practices. Yahoo's failure to take reasonable measures to secure the Account Information constitutes a prohibited practice because the representations that the defendants made to the Class Members in relation to the their security measures were false and misleading contrary to section 219, the particulars of which are as follows:

(a) at the time that the Class Members registered for their Yahoo Accounts, the defendants represented through the Contract that they would comply with their own privacy policy, *PIPEDA* and *PPIPS* and protect the Class Members' privacy, including their Account Information and the information contained in their Yahoo Accounts; and

(b) the defendants failed to disclose to the Class Members that their security measures were inadequate to secure the Class Members' privacy, including their Account Information and the information contained in their Yahoo Accounts.

63. As a result of the breaches of the *Consumer Protection Act*, the plaintiff pleads that the Class Members resident in Quebec have suffered damages for the false and misleading representations made to them by the defendants. In addition, Class Members resident in Quebec are entitled to punitive damages pursuant to s. 272 of the *Consumer Protection Act*.

E. Breach of confidence

64. The Class Members were invited to provide Account Information to the defendants, which the defendants then stored electronically on their computer network. The Class Members' Account Information was confidential, exhibited the necessary quality of confidence, was not public knowledge, and involved sensitive private details about the personal affairs of the Class Members.

65. The Class Members' Account Information was imparted to the defendants in circumstances in which an obligation of confidence arose, and in which the plaintiff and these Class Members could have reasonably expected their sensitive information to be protected and secured.

66. The defendants misused and made unauthorized use of these Class Members' Account Information by failing to make reasonable efforts to maintain confidentiality over the Account Information, to secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated information, in accordance with the defendants' own privacy policies, applicable laws and industry standards, as set out in paragraphs 27 to 46 of this Claim. The defendants' aforesaid misused and unauthorized use violated *PIPPS* and the *PIPEDA*, including sections 4.1, 4.5 and 4.7 of Schedule 1 to that legislation.

67. The defendants' misuse: resulted in unauthorized access and public disclosure of the Class Members' Account Information; likely resulted in unauthorized access and public disclosure of private information contained in the Class Members' Yahoo Accounts; and may possibly result in the future unauthorized access and public disclosure of private information contained in the Class Members' Yahoo Accounts, to the detriment of the Class Members. The defendants are therefore liable for the tort of breach of confidence.

F. Intrusion upon seclusion

68. The defendants were responsible for collecting, managing, storing, securing and/or deleting Class Members' Account Information.

69. By failing to take appropriate security safeguards/measures, as detailed above, the defendants are liable for the tort of intrusion upon seclusion, together with the anonymous hackers who intentionally invaded the Class Members' privacy.

70. The tort of intrusion upon seclusion is made out because:

(a) the anonymous hackers intentionally invaded the Class Members' privacy;

(b) the defendants' tortious conduct or alternatively recklessness facilitated the Hacker's ability to invade the Class Members' privacy;

(c) the Class Members' Account Information was invaded without lawful justification; and

(d) the Account Information that was invaded provided access to the Class Members' Yahoo Accounts, which contain highly sensitive and personal information and a reasonable person would consider the invasion of the Yahoo Accounts to be highly offensive causing anguish, humiliation or distress.

71. The defendants are liable for the past deliberate and significant invasions of the Class Members' privacy by the anonymous hackers and for any possible future such invasions because the cyberattacks causing the theft of the Class Members' Account Information fell within the ambit of risk that the defendants' enterprise created or exacerbated through failing to implement appropriate security measures as pleaded at paragraphs 27 to 46 of this claim. The defendants introduced the risk of the wrongs by collecting the Account Information and therefore should have managed and minimized the risk. A fair allocation of the consequences justifies imposition of liability on the defendants because there is a sufficient nexus between their wrongful acts and the Breach.

72. The cyberattacks, being the wrongful acts, were directly caused by the defendants' conduct in failing to implement appropriate security measures as pleaded in paragraphs 27 to 46 of this claim, such as to justify imposing liability in tort on the defendants for intrusion upon seclusion.

73. The defendants created or enhanced the risk of the cyberattacks occurring in that:

(a) the defendants provided the anonymous hackers with the opportunity to access Yahoo's internal computer network and data servers through inadequate and inappropriate security measures;

(b) the defendants created the opportunity for the anonymous hackers to carry out the cyberattacks by allowing unsecure access to the Account Information;

(c) the Class Members were vulnerable to the defendants' wrongful exercise of their powers to prevent a cyberattack and to the defendants' lack of appropriate security measures;

(d) the Class Members were vulnerable to the cyberattacks and to the release of their Account Information; and

(e) there is a significant connection between the risk created by the defendants in this situation and the cyberattacks.

74. The defendants acted with reckless indifference to the consequences of failing to maintain appropriate security measures at Yahoo, in the face of their duty to do so, and knew that they were consequently placing the Class Members at significant risk of a cyberattack.

75. The defendants were aware of the risk that certain consequences could result from a cyberattack but were indifferent to the risk. The defendants continuously failed to establish, maintain and enforce appropriate security measures and programs at Yahoo, despite the well-

known data security risks faced by a major technology company whose business was dependent on the collection of user information. The defendants' failure to implement appropriate security measures was an unreasonable risk to take and constituted reckless indifference.

76. The defendants' failure to implement appropriate security measures at Yahoo constituted either conscious wrongdoing or a marked departure from the standards by which responsible and competent technology companies in charge of large quantities of sensitive user information govern themselves in the collection, management, storage, securing and/or deleting of such data.

77. By failing to implement comprehensive, state-of-the-art security measures and appropriate security practices and procedures at Yahoo, the defendants knew their practices were not in conformity with the Yahoo Privacy Policy, *PIPPS*, the *PIPEDA*, or industry standards, and knew it was wrong to have done nothing or to decide not to do anything with reckless indifference to the consequences.

78. The defendants knew that they had a duty to act to improve Yahoo's security measures, practices and procedures and were aware that a failure to act could or would have the consequences of cyberattacks such as those which affected the Class Members, but decided not to do anything about it.

79. The failure to install and update appropriate security measures and programs at Yahoo was an unreasonable risk to take given that the very nature of Yahoo's business is based on collecting user information, and the resultant scope and amount of user information collected by Yahoo.

G. Publicity given to private life

80. The defendants were responsible for collecting, managing, storing, securing and/or deleting Class Members' Account Information. By failing to take appropriate security measures,

as detailed above, the defendants are liable for the tort of publicity given to private life, together with the anonymous hackers who intentionally invaded the Class Members' privacy.

81. The tort of publicity given to private life is made out because:

(a) due to the permanently and publicly available nature of information posted on the internet, the Class Members' Account Information was communicated to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge;

(b) the publication of the information in the Class Members' Yahoo Accounts would be highly offensive to a reasonable person and is not of legitimate concern to the public; and

(c) the defendants facilitated the anonymous hackers' ability to steal the Class Members' Account Information, publicize the Class Members' Account Information and/or sell the Class Members' Account Information on online black markets, and therefore to publicize the information in the Class Members' Yahoo Accounts.

82. The defendants are liable for the publication of the Class Members' Account Information by the anonymous hackers because the cyberattacks fell within the ambit of risk that the defendants' enterprise created or exacerbated through failing to implement appropriate security measures as pleaded at paragraphs 27 to 46 of this claim. The defendants introduced the risk of the wrongs by collecting the Account Information and therefore should have managed and minimized the risk. A fair allocation of the consequences justifies imposition of liability on the defendants because there is a sufficient nexus between their wrongful acts and the cyberattacks.

83. The publication of the Class Members' Account Information, being the wrongful act, was directly caused by the defendants' conduct in failing to implement appropriate security measures as pleaded in paragraphs 27 to 46 of this claim, such as to justify imposing liability in tort on the defendants for publicity given to private life.

84. The defendants created or enhanced the risk of the publication of the Class Members' Account Information occurring in that:

(a) the defendants provided the anonymous hackers with the opportunity to access Yahoo's internal computer network and data servers through inadequate and inappropriate security measures;

(b) the defendants created the opportunity for the anonymous hackers to carry out the cyberattacks by allowing unsecure access to the Account Information;

(c) the defendants failed to secure the Account Information itself, such that the anonymous hackers were able to fully publicize the Class Members' Account Information on the internet;

(d) the Class Members were vulnerable to the defendants' wrongful exercise of their powers to prevent a cyberattack from leading to the theft of unencrypted Account Information and to the defendants' lack of appropriate security measures;

(e) the Class Members were vulnerable to the cyberattacks and to the release of their Account Information; and

(f) there is a significant connection between the risk created by the defendants in this situation and the publication of the Class Members' Account Information.

H. Unjust enrichment/waiver of tort

85. The defendants generated profits by saving the costs of implementing appropriate cybersecurity measures, staffing and practices, policies and procedures. All defendants failed to incur the costs of equipment, consultants, technology, staffing and policy-making to comply with contractual obligations, reasonable standards of care and privacy legislation.

86. The defendants were unjustly enriched, with corresponding deprivation to the Class Members, and with no juristic reason. The defendants are therefore jointly and severally liable to the plaintiff and the other Class Members in waiver of tort to disgorge this financial gain to the benefit of the Class Members.

VII. DAMAGES

87. As a result of the defendants' wrongdoing, the Class Members have suffered damages including, but not limited to:

(e) damages to credit reputation;

(f) mental distress;

(g) costs incurred in preventing or rectifying identity theft or fraud;

(h) out-of-pocket expenses;

(i) wasted time, inconvenience, frustration and anxiety associated with taking precautionary steps recommended by Yahoo and to reduce the likelihood of identity theft, fraud or improper use of credit information; and

(j) time lost engaging in precautionary communications with third parties such as credit card companies, credit agencies, banks and other parties to take the steps recommended by Yahoo and to inform said third parties of the potential that the

Class Members' Account Information may be misappropriated and to resolve any delays thereby caused.

88. In addition, the Class Members have suffered or will likely suffer further damages from identity theft and/or fraud because the Account Information was, and remains, publicly available on the internet and may be downloaded and used for criminal purposes. It is likely or, alternatively, there is a real and substantial chance that the Account Information may be released on the internet or used in the future for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft and/or fraud, thereby causing the Class Members to suffer damages.

89. Class Members resident in Quebec have also suffered losses and damages for the defendants' breach of the *Consumer Protection Act*, as particularized above.

90. With respect to the claims for breach of contract, breach of confidence and intrusion upon seclusion and publicity given to public life, to the extent the amount of damages are uncertain, then the plaintiff and the other Class Members seek nominal damages for breach of contract and/or moral damages for breach of confidence, intrusion upon seclusion and publicity given to private life.

91. The defendants' conduct, as particularized above, was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, willful, and in complete disregard of the rights of the Class Members and, as such, renders the defendants liable to pay punitive damages.

VIII. STATUTES

92. The plaintiff plead and rely upon the *CJA*, the *CPA*, the *PIPEDA*, *PIPPS*, the *Consumer Protection Act*, the *Negligence Act*, R.S.O. 1990, c. N.1, and their regulations.

IX. THE PLACE OF TRIAL

93. The plaintiff proposes that this action be tried at the City of Toronto. Ontario is the appropriate venue because the Yahoo Canada Terms of Service includes a choice of jurisdiction provision which states that:

> The [Terms of Service] and the relationship between you and Yahoo shall be governed by the laws of the province of Ontario and Canada without regard to its conflict of law provisions. You and Yahoo agree to submit to the personal and exclusive jurisdiction of the courts located within the province of Ontario, Canada.

X. SERVICE OF FOREIGN DEFENDANTS

94. Pursuant to Rule 17.04(1), the plaintiff plead and rely upon Rules 17.02(a), 17.02(c), 17.02(f), 17.02(g), and 17.02(p) of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, in support of service of the Notice of Action and this Statement of Claim upon the defendant Yahoo outside of Ontario without a court order.

Date: January 16, 2017

CHARNEY LAWYERS PC
151 Bloor St. W., Suite 602
Toronto, ON M5S 1S4

Tel: (416) 964-7950
Fax: (416) 964-7416

Theodore P. Charney (LSUC #26853E)
Tina Q. Yang (LSUC #60010N)
Brendan O'Grady (LSUC #66419D)

Lawyers for the plaintiff

KARASIK Plaintiff	**v.**	**YAHOO! INC. and YAHOO! CANADA CO.** Defendants

Court File No. CV-16-566248-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding Commenced at Toronto

STATEMENT OF CLAIM
(Action Commenced by Notice of Action on December 16, 2016)

CHARNEY LAWYERS PC
151 Bloor Street West, Unit 602
Toronto, ON M5S 1S4

Theodore P. Charney (LSUC #26853E)
Tina Q. Yang (LSUC #60010N)
Brendan O'Grady (LSUC #66419D)

Tel: (416) 964-7950
Fax: (416) 964-7416

Lawyers for the plaintiff