



S 172962

NO. \_\_\_\_\_  
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

TWITCH INTERACTIVE, INC.

PETITIONER

AND:

SHAW COMMUNICATIONS INC.  
PAYPAL HOLDINGS INC.  
CLOUDFLARE, INC.  
WHOIS PRIVACY CORP.  
WHOIS GUARD, INC.

RESPONDENTS

**PETITION TO THE COURT**

**ON NOTICE TO:**

**SHAW COMMUNICATIONS INC.**  
c/o Attorney Office  
Doug McWilliams  
861 Cloverdale Avenue  
Victoria, BC V8X 4S7

**PAYPAL HOLDINGS INC.**  
c/o Attorney Office  
PO Box 49130  
2900 – 595 Burrard Street  
Vancouver, BC V7X 1J5

**CLOUDFLARE, INC.**  
c/o The Corporation Trust Company  
Corporation Trust Center 1209 Orange Street  
Wilmington, New Castle, DE 19801

21 MAR 17 17:06:51 R13H  
21 MAR 2017 17:29:62  
2017-03-31

**WHOIS PRIVACY CORP.**

c/o Agent Address  
Ocean Centre Montagu Foreshore  
East Bay Street  
New Providence, New Providence  
Nassau  
P.O. Box SS-19084  
Bahamas

**WHOIS GUARD, INC.**

P.O. Box 0823-03411  
Panama, Panama, PA

**This proceeding has been started by the Petitioner for the relief set out in Part 1 below.**

If you intend to respond to this Petition, you or your lawyer must

- (a) file a Response to Petition in Form 67 in the above-named registry of this court within the time for Response to Petition described below, and
- (b) serve on the Petitioner
  - (i) 2 copies of the filed Response to Petition, and
  - (ii) 2 copies of each filed Affidavit on which you intend to rely at the hearing

**Orders, including orders granting the relief claimed, may be made against you, without any further notice to you, if you fail to file the Response to Petition within the time for response.**

**TIME FOR RESPONSE TO PETITION**

A Response to Petition must be filed and served on the Petitioner,

- (a) if you were served with the Petition anywhere in Canada, within 21 days after that service,
- (b) if you were served with the Petition anywhere in the United States of America, within 35 days after that service,
- (c) if you were served with the Petition anywhere else, within 49 days after that service,  
or
- (d) if the time for response has been set by order of the court, within that time.

(1) **The address of the registry is:**

The Law Courts  
800 Smithe Street  
Vancouver, BC

(2) **The ADDRESS FOR SERVICE of the Petitioner is:**

McCarthy Tétrault LLP  
Barristers & Solicitors  
Suite 2400, 745 Thurlow Street  
Vancouver BC V6E 0C5

**Attention: Miranda Lam**

EMAIL address for service (if any):

mlam@mccarthy.ca

(3) **Name and office address of the Petitioner's lawyer:**

(same as above)

**CLAIM OF THE PETITIONER**

**PART 1. ORDER SOUGHT**

The Petitioner seeks the following orders:

1. Within 30 days of service of the Order, Shaw Communications Inc. ("**Shaw**") shall produce to the Petitioner's solicitor the name(s), street address(es), email address(es), additional IP address(es), and any other identifying information of the customer associated with IP address 70.68.65.141 assigned March 24, 2017 at 03:34:31 and March 21, 2017 at 21:51:58 (the "**Shaw Information**");

2. Within 15 days of service of the Order, PayPal Canada Co. ("**PayPal**") shall produce to the Petitioner's solicitor the name(s), street address(es), email addresses, IP address(es), and any other identifying information of the customer associated with chatsurge.net, feelmorebirds@gmail.com, or obnoxious@dongcorp.org (the "**PayPal Information**");

3. Within 15 days of service of the Order, CloudFlare, Inc. Inc. ("**CloudFlare**") shall produce to the Petitioner's solicitor the name(s), street address(es), email addresses, IP address(es), and any other identifying information associated with Chatsurge.net (the "**Cloudflare Information**");
4. Within 15 days of service of the Order, Whois Privacy Corp. ("**Whois Privacy**") shall produce to the Petitioner's solicitor the name(s), street address(es), email addresses, IP address(es), and any other identifying information associated with Chatsurge.net (the "**Whois Privacy Information**");
5. Within 15 days of service of the Order, WhoisGuard, Inc. ("**WhoisGuard**") shall produce to the Petitioner's solicitor the name(s), street address(es), email addresses, IP address(es), and any other identifying information associated with the email address obnoxious@dongcorp.org. (the "**WhoisGuard Information**");
6. The Petitioner shall pay to Shaw all reasonable costs incurred by Shaw for the retrieval of the Shaw Information, fixed at \$250.00;
7. The Petitioner shall pay to PayPal all reasonable costs incurred by PayPal for the retrieval of the PayPal Information;
8. The Petitioner shall pay to CloudFlare all reasonable costs incurred by CloudFlare for the retrieval of the CloudFlare Information;
9. The Petitioner shall pay to WhoisPrivacy all reasonable costs incurred by WhoisPrivacy for the retrieval of the WhoisPrivacy Information;
10. The Petitioner shall pay to WhoisGuard all reasonable costs incurred by WhoisGuard for the retrieval of the WhoisGuard Information;
11. The Petitioner is entitled to use the information sought from and provided by the Respondents in any subsequent proceedings; and

12. Such further and other relief as counsel may request and this Honourable Court deems just.

## **PART 2. FACTUAL BASIS**

1. The Petitioner, Twitch, is a Delaware corporation with its principal place of business in San Francisco, California. Twitch is a leading social video platform for video game-related content that allows users to broadcast gaming-related content (“**Broadcasters**”) as part of a social, interactive community.

2. The Respondent, Shaw, is a telecommunications company extra provincially registered in British Columbia, with its head office in Calgary, Alberta.

3. The Respondent, PayPal is a corporation that provides worldwide online payments services. PayPal is extra provincially registered in British Columbia, with its head office in Halifax, Nova Scotia.

4. The Respondent, CloudFlare, is a corporation that provides a content delivery network, internet security services and distributed domain server services. CloudFlare is a Delaware corporation, with its head office in San Francisco, California, USA. Websites utilizing CloudFlare’s servers and services are accessible in British Columbia.

5. The Respondent, Whois Privacy, is a company with a registered office in the Bahamas.

6. The Respondent, WhoisGuard, is a company registered in the Republic of Panama.

### **The Twitch Platform**

7. As a leading social video platform for video game-related content, Twitch allows its users and Broadcasters to engage with each other through, among other things, live streaming video and chat (the “**Twitch Services**”). Users from around the world can watch the broadcasts that interest them (“**Viewers**”), and chat with the Broadcasters and other users while watching the broadcast. Twitch attracts and retains its users by providing high quality content. It hosts more than 2 million unique Broadcasters and 100 million unique Viewers per month.

8. Each Broadcaster has a distinct broadcasting channel on Twitch (“**Channel**”), where they stream live video that other Twitch users can view alongside a chat window for Viewers to participate in live text chat while watching the broadcast.

9. High quality content and user experiences are paramount to attracting and retaining users. To encourage and incentivize Broadcasters to create and provide excellent content, Twitch has a Partnership Program which compensates selected broadcasters. Through this program, Twitch shares revenue with qualifying broadcasters, enabling numerous broadcasting Partners to earn a living through their exceptional efforts in creating content on Twitch.

10. Broadcasters work hard to create attractive Channels and build their personal brands. The best Broadcasters become Twitch Partners and are often celebrities in the gaming community. These Broadcasters are not only excellent gamers, but also are engaging and entertaining. In this way, Broadcasters work extensively to create and foster authentic, passionate and loyal communities on Twitch. They also interact with their audience by participating in chat, running promotions, and fundraising for charitable causes. Broadcasters have the opportunity to earn revenue through products offered by Twitch, including products available solely through Twitch’s chat service, as well as through advertisements and sponsorships, all of which depend on the brand and reputation of the Broadcaster's channel and chat.

### **The Twitch Terms and Conditions**

11. All users who access the Twitch Services must agree to be bound by, among other things, Twitch’s Terms of Service (the “**Terms**”) and Twitch’s Community Guidelines (the “**Guidelines**”). The Terms specifically provide:

The Terms of Service apply whether you are a user that registers an account with the Twitch Services or an unregistered user. You agree that by clicking “Sign Up” or otherwise registering, downloading, accessing or using the Twitch Services, you are entering into a legally binding agreement between you and Twitch regarding your use of the Twitch Services. You acknowledge that you have read, understood, and agree to be

bound by these Terms of Service. If you do not agree to these Terms of Service, do not access or otherwise use any of the Twitch Services.

12. Further, the Terms expressly prohibit a user from, among other things:

- (a) creat[ing], upload[ing], transmit[ing], distribut[ing], or stor[ing] any content that is inaccurate, unlawful, infringing, defamatory, obscene, pornographic, invasive of privacy or publicity rights, harassing, threatening, abusive, inflammatory, or otherwise objectionable;
- (b) mak[ing] unsolicited offers, advertisements, proposals, or send[ing] junk mail or spam to users of the Twitch Services...;
- (c) defam[ing], harass[ing], abus[ing], threaten[ing] or defraud[ing] users of the Twitch Services...;
- (d) interfer[ing] with or damag[ing] operation of the Twitch Services or any user's enjoyment of them, by any means, including uploading or otherwise disseminating viruses, adware, spyware, worms, or other malicious code;
- (e) access[ing] any website, server, software application, or other computer resource owned, used and/or licensed by Twitch, including but not limited to the Twitch Services, by means of any robot, spider, scraper, crawler or other automated means for any purpose, or bypass any measures Twitch may use to prevent or restrict access to any website, server, software application, or other computer resource owned, used and/or licensed Twitch, including but not limited to the Twitch Services;
- (f) interfer[ing] with or disrupt[ing] the Twitch Services or servers or networks connected to the Twitch Services, or disobey[ing] any requirements, procedures, policies or regulations of networks connected to the Twitch Services; us[ing] the Twitch Services in any manner that could interfere with, disrupt, negatively affect or inhibit other users from fully enjoying the Twitch Services, or that could damage, disable, overburden or impair the functioning of the Twitch Services in any manner; and
- (g) attempt[ing] to circumvent any content filtering techniques we employ, or attempt to access any service or area of the Twitch Services that you are not authorized to access.

13. The Guidelines, which govern the conduct of all those using Twitch's services, specifically provide that:

(a) Any content or activity that disrupts, interrupts, harms, or otherwise violates the integrity of Twitch services or another user's experience or devices is prohibited. Such activity includes:

(i) Posting large amounts of repetitive, unwanted messages or user reports

And:

(b) Any content or activity that facilitates, promotes, or encourages discrimination, harassment, or violence based on race, ethnicity, gender identity, sexual orientation, age, disability, religion, or nationality is prohibited.

14. The Spambot Attacks, described below, violate the Twitch Terms and Guidelines.

### **The Spambot Attacks**

15. On or about February 24, 2017, Twitch became aware of malicious spambot flooding several Broadcasters' public chat with repetitive messages (the "**First Spambot Attack**"). A spambot is a computer program used to send unsolicited messages (or "spam") via email or other online forums. The First Spambot Attack rendered the public chat feature for each attacked Broadcaster's channel unusable and disrupted the Broadcaster's stream. The volume of spam messages on the attacked channels was enormous. The bots were posting an average of 34 spam messages per minute while on some channels the rate was 699 messages per minute. These attacks had a detrimental impact on Twitch's core value proposition, which is a shared, real-time experience, as well as a potentially detrimental financial effect for both the Broadcaster and Twitch.

16. As soon as it became aware of the First Spambot Attack, Twitch launched an immediate investigation and took steps towards remediation (the "**Investigation**"). To date, the Investigation has consumed nearly 200 hours of Twitch employee time. While Twitch was able to stop the First Spambot Attack, as of March 24, 2017, the flooding has resumed (the "**Second Spambot Attack**", together with the First Spambot Attack, the "**Spambot Attacks**"). The Second Spambot Attack is ongoing.

17. To date, over 1,000 channels have been attacked with over 150,000 spam messages.



18. Twitch has received over 375 individual user reports regarding spam messages containing racism, homophobia, sexual harassment, false implications of viewbotting and soliciting child sex exploitation material. Examples of these spam messages include the following:

- (a) 2017-02-25 07:51:43 PM PST #franplayshalo (5690948) 26281575590585 (148811527) We wanna see gameplay not those big jugs 461088458 237152027
- (b) 2017-02-24 07:37:30 PM PST #emmalayne (124069501) 34653269065018 (148673456) Lemme eat dat puss 161138767
- (c) 2017-02-26 12:19:56 PM PST #budderkingisback (86062929) 26619574507648 (148897840) Death to all jews Death to all jews Death to all jews Death to all jews Death to all jews Death to all jews Death to all jews 259494252
- (d) 2017-02-26 01:01:18 PM PST #the8bitterterrorist (62453963) 81786656657927 (148892820) Allah hates Gays KappaPride 484676295
- (e) 2017-02-26 12:36:38 PM PST #helenalive (41343682) 81786656657927 (148892820) TriHard N I G G E R TriHard 774581289
- (f) 2017-02-25 08:31:05 PM PST #ballerr65 (73131992) 11843282414220 (148811376) Get the black guy outta here. What a \*\*\* 214379053 188628588
- (g) 2017-02-25 08:23:11 PM PST #crunk\_muffin (72142123) 11843282414220 (148811376) @Wolfyy Trade cp? 978828276 121965617

### **Identity of the Attacker**

19. Through the course of the Investigation, Twitch discovered that the Spambot Attacks originate from the website [www.chatsurge.net](http://www.chatsurge.net) (“Chatsurge.net”).

20. Chatsurge.net also includes a link to a YouTube tutorial video (the “YouTube Tutorial”) posted on the YouTube channel for username “Ob Nox”. The linked video shows how the spambot attack offered on Chatsurge.net works. As demonstrated in the YouTube Tutorial, users

who have paid to create accounts (using PayPal or Bitcoin), can launch attacks against the Twitch channel of their choosing.

21. Through the Investigation and described further below, Twitch has uncovered the following identifying information about the individual it believes to be the perpetrator:

- (a) Email address: [obnoxious@dongcorp.org](mailto:obnoxious@dongcorp.org);
- (b) YouTube video found via a link on [chatsurge.net](http://chatsurge.net) posted by “Ob Nox”;
- (c) Thread originated by “obby” on [HackForums.net](http://HackForums.net) found via a link on [chatsurge.net](http://chatsurge.net);
- (d) Shaw Communications Inc. (“**Shaw**”) IP address 70.68.65.141, located in Coquitlam, B.C.; and
- (e) PayPal accounts associated with the email [feelmorebirds@gmail.com](mailto:feelmorebirds@gmail.com).

22. Twitch is unable to uncover additional identifying information.

23. Further information is required from the Respondent service providers in order to determine the identity of the person associated with these accounts and these are the only practicable sources of information available.

24. [Chatsurge.net](http://Chatsurge.net) also includes a link to a thread on [hackforums.net](http://hackforums.net) originated by “obby” that advertises spambot services, as well as his efforts to bypass the defences Twitch put in place (and described further below).

25. The attacking bots all had [@mailnesia.com](mailto:@mailnesia.com) addresses associated with their Twitch accounts. When Twitch engineers blocked accounts with those addresses from accessing the “chat” feature on various channels, [Chatsurge.net](http://Chatsurge.net) was taken down and replaced with a message saying the bots were disabled due to a change on Twitch.

26. [Chatsurge.net](http://Chatsurge.net) was then updated, indicating the bot account emails were being switched to Gmail, which is an email service developed by Google. The Spambot Attack resumed on March

2, 2017. When the flooding resumed at this time, Twitch noticed that the new bots were all associated with Gmail accounts.

27. In the course of the Investigation, Twitch also determined that the attacker broadcast himself working on his bot software. Very shortly after that broadcast, Chatsurge.net was updated to offer that software. The attacker was associated with a Shaw IP address, namely 70.68.65.141. This IP address is located in Coquitlam, BC, Canada, and it is believed that the perpetrator of the Spambot Attacks is located in the same place as this IP address.

28. The PayPal account associated with Chatsurge.net uses the email address feelmorebirds@gmail.com.

### **Shaw Communications Inc.**

29. By using Shaw's services, customers agree to be bound by Shaw's Acceptable Use Policy. Shaw customers are prohibited from disseminating hateful material. In this regard, Shaw's Acceptable Use Policy - Internet, states the following:

Use of the Services for any activity that violates Local, Provincial, Federal or International law, order or regulation, is a violation of this Agreement. Prohibited activities include, but are not limited to:

1. Posting, storing, transmitting or disseminating unlawful material, including without limitation, child or other pornography, any content, data or other material which is libelous, obscene, hateful, unlawful, threatening, ethnically offensive, defamatory or which in any way constitute or encourages conduct that would constitute a criminal offense.

...

You hereby authorize Shaw to cooperate with (i) law enforcement authorities in the investigation of suspected criminal violations, and/or (ii) system administrators at other Internet service providers or other network or computing facilities in order to enforce this Agreement. Such cooperation may include Shaw providing the username, IP address, or other identifying information about a subscriber, in accordance with the guidelines set out in Shaw's Privacy Policy.

30. Furthermore, Shaw's Privacy Policy provides:

3.4.1 Shaw may disclose Customer's Personal Information to:

...

g. a third party, where the Customer has given Shaw consent to such disclosure or if disclosure is permitted or required by law, in accordance with PIPEDA.

### **PayPal Canada Co.**

31. By using PayPal's services, customers agree to be bound by PayPal's Acceptable Use Policy. Under this policy, PayPal customers are prohibited from disseminating hateful material:

You may not use the PayPal service for activities that:

1. violate any law, statute, ordinance or regulation.
2. relate to transactions involving ... (d) items that encourage, promote, facilitate or instruct others to engage in illegal activity, (e) stolen goods including digital and virtual goods, (f) the promotion of hate, violence, racial intolerance or the financial exploitation of a crime, (g) items that are considered obscene... (i) certain sexually oriented materials or services ...

32. Furthermore, PayPal's Privacy Policy provides:

We may share your personal information we collect from you, including your name, contact details, and transactions and activities, with:

... other third parties pursuant to a subpoena, court order, or other legal process or requirement applicable to PayPal or one of its affiliates; when we need to do so to comply with law or credit card rules; or when we believe, in our sole discretion, that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our User Agreement.

### **CloudFlare, Inc.**

33. CloudFlare is the server host of both Chatsurge.net and HackForums.net

34. By using CloudFlare’s services, customers agree to be bound by CloudFlare’s Privacy Policy, which provides:

It’s possible that we may be required by law, court order, or other legal process to provide information about our customers to outside parties. It’s our policy to ensure adherence to the due process of law in all such instances, and if we are required to provide information under these circumstances, we will, whenever possible, attempt to inform users whose information we are compelled to produce, unless prohibited by law.

We may also retain copies of personal information to comply with our legal obligations, pursuant to our data retention policies, or for such reasonable period as is required to address potential disputes.

### **Whois Privacy and WhoisGuard**

35. Chatsurge.net and Dongcorp.org are registered to WhoisPrivacy and WhoisGuard, whose registrations show locations in the Bahamas and Panama, respectively, which is an attempt to anonymize the entity or individual to whom the domain name is truly registered.

## **PART 3. LEGAL BASIS**

### **Equitable Bill of Discovery: The “Norwich Pharmacal Order”**

1. This Court has inherent jurisdiction to grant an “equitable bill of discovery” (or *Norwich* order). The remedy permits a court to order discovery against a person who the applicant has no cause of action against, and who is not a party to an action. The order requires the third party to provide full information necessary to advance a claim.
2. The remedy of an equitable bill of discovery is available in British Columbia: *Kenney v. Loewen*, (1999), 64 B.C.L.R. (3d) 346 (S.C.) [*Kenney*]; and *College of Opticians of British Columbia v. Coastal Contacts Inc.*, 2010 BCSC 104, both citing *Norwich Pharmacal Co. v. Commissions of Customs and Excise*, [1974] A.C. 133 (H.L.).

3. The British Columbia Supreme Court considered the nature and scope of *Norwich* orders in *Equustek Solutions Inc. v. Jack*, 2014 BCSC 454 [*Equustek #1*]. In *Equustek #1*, the plaintiff sought the production of documents held by a non-party, the Toronto Dominion Bank, relating to the recipients of payments from certain bank accounts.

4. Mr. Justice Abrioux, following the Ontario Court of Appeal in *GEA Group AG v. Ventra Group Co*, 2009 ONCA 619, adopted a broad and dynamic formulation of the remedy, stating:

[10] The principle underlying such equitable discovery is that:

... where discovery is absolutely necessary in order to enable a party to proceed with a bona fide claim, it is the duty of the Court to assist with the administration of justice by granting an order for discovery, unless some well-founded objection exists against the exercise of such jurisdiction.

[11] *Norwich* orders have been granted in numerous situations, including:

- (i) where the information sought is necessary to identify wrongdoers;
- (ii) to find and preserve evidence that may substantiate or support an action against either known or unknown wrongdoers; or even
- (iii) to trace and preserve assets.

See *GEA* at para. 51.

5. The Court ultimately ordered TD to provide the identity of individuals and associated documents to the applicant.

6. The Court in *Equustek #1* enumerated the factors to be considered on an application for a *Norwich* order:

- (a) Whether the applicant has provided evidence sufficient to raise a valid, *bona fide* or reasonable claim;

- (b) Whether the applicant has established a relationship with the third party from whom the information is sought such that it establishes that the third party is somehow involved in the acts complained of;
- (c) Whether the third party is the only practicable source of the information available;
- (d) Whether the third party can be indemnified for costs to which the third party may be exposed because of the disclosure, some [authorities] refer to the associated expenses of complying with the orders, while others speak of damages; and
- (e) Whether the interests of justice favour the obtaining of that disclosure.

### **The Applicant has Raised a Valid, Bona Fide Claim**

7. The Petitioner has a *bona fide* case of breach of contract against the perpetrator of the Spambot Attacks as the attack is in clear violation of Twitch's Terms and Guidelines, and has caused and continues to cause Twitch loss and damage. Since the Spambot Attacks began, Twitch has devoted hundreds of hours to resolving the issue, and the attacks continue, undermining its brand.

8. In addition, the Petitioner has a *bona fide* case against the perpetrator of the Spambot Attacks for the tort of unlawful interference with economic relations as the perpetrator intentionally interfered with the broadcasts of Broadcasters with the intent to cause harm.

9. The disclosure of the information requested from the Respondents will facilitate rectification of the wrong committed by providing the identity of the perpetrator of the Spambot Attacks.

### **The Respondents are Involved in the Spambot Attacks**

10. Shaw is involved in the wrongful conduct of the perpetrator as it appears someone had tested the spambots on Twitch, and this test is associated with a Shaw IP address, namely 70.68.65.141.

11. PayPal is involved in the wrongful conduct of the perpetrator as it provided the means for the perpetrator to collect fees from the Spambot Attacks.

12. Cloudflare is involved in the wrongful conduct of the perpetrator as it provided the means for the perpetrator to advertise the Spambot Attacks by providing the server that hosts the ChatSurge.net website.

13. By shielding the identities of the owners of the domain names chatsurge.net and dongcorp.org, WhoisPrivacy and WhoisGuard are providing a means for the perpetrator to don the cloak of anonymity to undertake this harmful conduct.

**The Respondents are the Only Practicable Source of Information Available**

14. There is no other practicable way for the Petitioner to obtain the identity of the perpetrator of the Spambot Attack. Twitch has already exhausted all the means available to it in this regard. Moreover, counsel for the Petitioner has requested the disclosure of identifying information from Shaw, PayPal, and CloudFlare. Shaw and Cloudflare have indicated that a court order is required for disclosure.

**The Respondents Will be Indemnified**

15. The Petitioner has agreed to pay the reasonable fees incurred by the Respondents for retrieval and production of the information requested.

**The Interests of Justice Favour Granting the Norwich Order**

16. The Petitioner is seeking the identity of an attacker who has infiltrated its systems, compromised its services, and caused financial and reputational harm, both to the Petitioner and its users. Any user of the services offered by the Respondents to perpetrate illegal activity can have no expectation of privacy.

17. Federal and provincial law authorizes the disclosure of personal information, without user consent, pursuant to a court order. (See section 7(3)(c) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, and section 18(1)(i) of the *Personal Information Protection Act*, S.B.C. 2003, c. 63.)



18. The Respondents' respective privacy policies also provide for the disclosure of personal information where required by law. For example, Shaw's Privacy Policy states:

3.4.1 Shaw may disclose Customer's Personal Information to:

...

g. a third party, where the Customer has given Shaw consent to such disclosure or if disclosure is permitted or required by law, in accordance with PIPEDA.

19. PayPal's Privacy Policy states:

We may share your personal information we collect from you, including your name, contact details, and transactions and activities, with:

... other third parties pursuant to a subpoena, court order, or other legal process or requirement applicable to PayPal or one of its affiliates;

20. CloudFlare's Privacy Policy states:

It's possible that we may be required by law, court order, or other legal process to provide information about our customers to outside parties. It's our policy to ensure adherence to the due process of law in all such instances, and if we are required to provide information under these circumstances, we will, whenever possible, attempt to inform users whose information we are compelled to produce, unless prohibited by law.

### **Jurisdiction of the Court**

21. This Court has jurisdiction to make orders against CloudFlare, WhoisPrivacy and WhoisGuard who carries on business in the province through online activities. This Court has the jurisdiction to make orders that have an extraterritorial effect (see: *Equustek Solutions Inc. v. Jack*, 2015 BCCA 265 at paras. 54-56, 90, aff'g 2014 BCSC 1063, leave to appeal to SCC granted, 2016 CanLII 7602 (Appeal heard 6 December 2016; Judgment reserved)).

**PART 4. MATERIALS TO BE RELIED ON**

1. Affidavit #1 of Zach Goodman, sworn March 30, 2017;
2. Affidavit #1 of Katerina Doumakis, sworn March 31, 2017; and
3. Such further and other material as counsel may advise and the Court may permit.

The Petitioner estimates that the hearing of the Petition will take **25 minutes**.

DATED: March 31, 2017

  
\_\_\_\_\_  
MIRANDA LAM  
Counsel for the Petitioner