Court File No.: T-2058-12

FEDERAL COURT

BETWEEN:

VOLTAGE PICTURES LLC

PLAINTIFF/MOVING PARTY

- and -

JOHN DOE and JANE DOE

DEFENDANTS

- and -

TEKSAVVY SOLUTIONS INC.

RESPONDING PARTY

- and -

SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

INTERVENOR

AFFIDAVIT OF TIMOTHY LETHBRIDGE

I, Timothy Lethbridge, of the City of Ottawa in the Province of Ontario, AFFIRM THAT:

I. Background and Qualifications

1. I am a full professor of software engineering and computer science at the

University of Ottawa. I am also a licensed Professional Engineer, and a registered Information Systems Professional. These are professional designations under Ontario law.

2. My qualifications are:

a) I have taught at the university level since 1986;

b) I received a Bachelor of Science in Computer Science from the University of New Brunswick in 1985 and an MsC(CS) from the same University in 1987. I received my Ph.D. in computer science in 1994 from the University of Ottawa;

c) I have written a widely-used textbook on Software Engineering, published by McGraw Hill;

d) I have published over 100 peer-reviewed papers in software engineering;

e) one of my main teaching and research focuses is design of software in which several computers communicate with each other;

f) another teaching focus is professionalism, in which I teach students about intellectual property and file sharing, among many other topics; and

g) I have studied the BitTorrent protocol, for the purpose of teaching about it. I have read peer-reviewed publications relating to it, and have maintained a long-time professional interest in its functionality.

II. IP addresses

1. An Internet Protocol Address ("IP address") is a numerical identifier assigned to a device so as to allow it to communicate with other devices via Internet Protocol.

2. Internet Service Providers ("ISPs") assign IP addresses to their customers' networks. The method can vary depending on the type of connection (e.g. DSL, cable, cellular, WiFi). Each ISP has a pool of IP addresses from which they can draw, and each assignment is subject to change.

3. While an IP address for a device connected to the public Internet is unique, it is not necessarily associated with any one computer, nor, obviously, with any one individual computer user. Multiple computers or devices within a home or corporate network routinely share a single IP address. In other words, to other computers on the Internet, these multiple individual users would appear to be the same device since they would all share a single IP address. For example, a coffee shop might offer complimentary wireless Internet. communications for customers. Communications from laptops and other mobile devices thereby connected to the Internet would usually appear to be originating from the same IP address.

4. This sharing of a single IP address for use within a network is performed using a protocol called Network Address Translation (NAT). Since worldwide there is an extreme shortage of available IP addresses, the use of NAT has become standard.

5. Alternatively, at any given moment, a particular IP address may not have been assigned by an ISP.

6. To determine which device was associated with an IP address at a given moment in time, it is critical that the time provided is accurate. This is because the timekeeping devices in computers are prone to drifting out of sync. This includes both the computers of the ISP and a computer associated with the plaintiff's tracking software. Computer clocks can drift by many seconds if not properly reset. Without evidence from the plaintiff and ISP as to the exact amount of drift their computers experienced at a particular time, it is impossible to be certain of the specific computer or network using a specific IP address at that moment. This is because IP addresses can be instantly reassigned from one connection to another.

7. Regardless of whether the connected device or network can be determined, an IP address can not be relied on to identify an individual Internet user. Accordingly, behaviour observed or communications identified over the Internet and associated with a particular IP address cannot be attributed to any particular individual, including the subscriber paying for the account. There are many reasons for this.

8. First, for most home and office users of the Internet, the IP address that serves their network tends to be fixed for extended periods. However, unless people have paid for a static IP address, ISPs can change an IP address whenever they feel like, although this normally only happens after extended periods (days or weeks) of inactivity. There is a shortage of IP addresses so this is happening more often.

9. Second, people can explicitly release their IP address. If they then wait a while before reconnecting their service, they are likely to get a different IP

address.

10. Third, if people maintain an open WiFi network, neighbours might use their network. An open WiFi network requires no password. Anyone within range of the network may connect their WiFi enabled device to that network. Their online communications and behaviour will then be associated with the IP address of the owner of the open WiFi network. The owner of the open WiFi network could have no knowledge whatsoever of such connections.

11. Fourth, even with respect to closed WiFi networks, it is routine for visiting friends and relatives to ask for and be given a person's WiFi password so they can connect their mobile devices or laptop to the Internet while visiting. Sharing WiFi passwords with visitors allows playing of games, checking email and many other routine daily tasks. This is just as normal as asking to use the phone and is almost a necessity of life now. However, that means i) visitors can use any service through the homeowner's WiFi network, and ii) the owner of the WiFi network has lost control over the password. Visitors may share the password with others without the knowledge or permission of the WiFi network owners, permitting third parties to use the WiFi network without the knowledge of the network owner.

12. Fifth, all household members likely share the same IP address, using Network Address Translation internally in the home to share a single Internet connection among numerous computers and mobile devices. Accordingly, roommates, children, and other household members might use online services completely

unbeknownst to the individual who actually subscribes to and pays for the Internet service.

13. Sixth, people can use anonymizing services, and Virtual Private Networks (a "VPN") to make it look as though access to a service is coming from somewhere else. This is not done just to evade surveillance that may be able to otherwise determine your IP address. It can be done as a requirement to access certain services that are 'bound' to certain IP ranges. I often connect to the University's VPN to access library services. But there are public VPN services too that serve many useful purposes including helping protesters in non-democratic countries in their struggle for democracy and human rights and protecting anonymity of news sources and whistle-blowers. The IP address you get when connecting to a VPN will change, and may be behind a NAT router, so may be shared with others.

14. Seventh, more and more people are using Internet service over the cellular network (known as 'tethering'). The IP address used for this can change every time you connect, and hence multiple times in a day. In my house, for example, we have two cellular services and one land line service. So the above problems can be multiplied – it is possible your neighbour who knows your WiFi password used by your phone for tethering could access a service such as BitTorrent though that, at least for a short while.

15. Finally, malware (such as botnets) can route traffic through other computers in a manner that is unknown to the owner of that computer. In this way, third parties may surreptitiously infect a home or business computer to engage in unlawful or

malicious behaviour. All such online behaviour and communications will be associated with the IP address of the compromised home or office network or computer. The owner of the compromised network or computer will have no knowledge of such behaviour.

16. If something wrongful is alleged to have happened through an IP address it would be impossible to conclude that any one individual was responsible without additional evidence obtained by examining the actual computers involved.

17. I have many times found out that, when accessing cellular IP networks, I am locked out of certain services because the service has flagged my IP as a risk (e.g. it has previously been used by hackers). If you are allocated such an IP address, others may think your legitimate email is spam for example. Spammers rely on changing IP addresses to evade anti-spam software. So do hackers that want to try and crack passwords: They need to make each distinct 'crack' attempt (failed password entry) look like it was from a different random person.

III. BitTorrent

18. BitTorrent is a file-sharing protocol. It is particularly popular method to distribute large files.

19. To facilitate sharing, the file to be shared is divided in to many smaller pieces. Users (known as "Peers") can share those pieces, which they have provided or have already downloaded from other peers, hence the term "peer-to-peer". This has the advantage that no one computer necessarily bears the full burden of

serving all those users interested in obtaining a file.

20. A person who wishes to share a file will create a Torrent file. The Torrent contains several fields including: a description of the file to be shared; a cryptographic description of the Torrent file itself (an "Info-hash"); a cryptographic description of each individual piece so as to ensure file integrity; and a list of "Trackers", which are a third-party computers that coordinate communication between Peers. The Torrent file does not contain any portion of the file to be shared.

21. When a user wishes to download a file he or she will obtain the Torrent file, usually by clicking on a link in a web browser. When the Torrent is opened with the appropriate client program, the user's device will attempt to connect to the listed Trackers.

22. Once connected, the Tracker will announce to existing Peers that the user has become a Peer. At this point the newly-connected Peer does not possess any portion of the shared file.

23. Once the user has been announced as a Peer, the user begins downloading portions of the shared file from other Peers identified by the Tracker file. Participants in this transaction, known as a "swarm", may download and upload portions of content at the same time. Thus, one may not have downloaded the complete file before another peer in the swarm uploads a portion of the file from one's computer.

24. One feature of the BitTorrent protocol is that users do not spontaneously upload those pieces of a given file in their possession. Instead, they wait for requests from other peers. It is possible to configure a BitTorrent client to refuse such requests, although this will affect download performance as most BitTorrent client software is designed to discourage sharing with those who do not themselves share.

25. BitTorrent is used legitimately to help distribute content you have created (or have a license to), and want others to access. Such content may include a software application you have developed, a Linux operating system distribution, an indie movie licensed under a permissive license such as a Creative Commons license, your book, your family photo album, or sound recordings of your band. However unless you pay for an expensive hosting service, you don't have a lot of bandwidth with which to permit this access. Without BitTorrent, you might get huge numbers if 'hits' (downloads) that would overload your network and computer. By making that content available for others' access via BitTorrent, you permit an essentially random set of other BitTorrent participant computers to share the load when people want to download your material. Other participants (and you don't know who they are in general, since the swarm can grow to include any of many millions of computers) thus make use of your computer, and you make use of their computers once they have started to download (i.e. become a 'peer' of) your material.

26. It is common practice help other parties share their content by becoming a peer of

their content. Being a good peer for others' content will encourage them to become a peer for the content you wish to distribute.

27. The BitTorrent protocol makes excellent use of scarce resources (the relatively narrow Internet 'pipe' to your computer and to others in the swarm).

28. Identification of individuals involved in a swarm is not possible merely from the data one might extract from an examination of the Internet connection data of participants in a swarm. One may identify the IP address used by a participant in a swarm. For the reasons given in the preceding section of this affidavit, one cannot identify individuals reliably by IP address. IP addresses can point to Internet subscribers, but do not identify individuals.

29. Moreover, people who want to hide their online activity have many ways to do so. I have described some of these above:

    a. one may use another's open WiFi connection (such as a neighbour's or an Internet café's),

    b. one may switch IP address though various means,

    c. one may use anonymizers such as proxy services and VPNs;

    d. one may use a friend's Internet access, and

    e. one may participate in botnets to use others' computing resources and Internet connections..

30. BitTorrent uses certain software architecture techniques that are used in many

types of software, including store and forward, caching and load balancing:

31. "Store and forward" simply refers to the fact that in almost all cases, when moving data around, it has to be stored, hence making a copy. This happens in routers and internally in every computer.

32. "Caching" means that a temporary backup copy is kept to avoid having to go back to the original source for the data if it is needed again. This is done in almost every movement of data in computers and networks. ISPs have caches of web pages, for example.

33. "Load balancing" means distributing work over many computers. All large websites have to do this. When you get a page from CNN or Google, for example, your request is routed to one of many computers distributed around the world. BitTorrent simply does load balancing over a variety of computers owned by the public, instead of under the control of one enterprise. It caches the data on those servers, as happens in any load balancing approach. So BitTorrent is really just like normal web publishing except that it uses public load balancing.

34. As with normal web downloading, people may accidentally download material they do not intend to download using BitTorrent or may be tricked into downloading material they think is legitimate (by spam emails for example). It has been found that a large fraction of BitTorrent files are contaminated by malware; users clearly do not want or intend to download such malware, but are tricked into doing so. The same thing can happen with copyright material because

the original uploaders want to promote distribution.

35. Users may also not know what material is in a torrent until they download it and look at it. They may at that point choose to delete it, but during the download process they nonetheless will have helped participate in the further distribution of the material as described above.

36. If someone wants to make "fair use" of or "fair dealing" with material by looking at a small part of it, or conducting research into it, they nonetheless will normally have to wait for the entire file to finish downloading, since most content viewing software applications will not open a file until it is complete. Once again, while this downloading is happening, the BitTorrent protocol will also be helping distribute the material to others.

37. I make this affidavit in support of CIPPIC's intervention in the moving party's Rule 36 motion, and for no other purpose.

SWORN before me at the City of)
Ottawa in the Province of Ontario)
this 27th day of February, 2013.) Timothy Lethbridge

David Fewer, Commissioner for Taking Oaths