Court File No. T-955-21

FEDERAL COURT

B E T W E E N:

ROGERS MEDIA INC.
ROGERS COMMUNICATIONS INC.
BCE INC.
BELL MEDIA INC.
CTV SPECIALTY TELEVISION ENTERPRISES INC.
THE SPORTS NETWORK INC.
LE RESEAU DES SPORTS (RDS) INC.
GROUPE TVA INC.

Plaintiffs

- and -

JOHN DOE 1
JOHN DOE 2
OTHER UNIDENTIFIED PERSONS WHO OPERATE UNAUTHORIZED STREAMING SERVERS PROVIDING ACCESS TO NHL LIVE GAMES IN CANADA

Defendants

- and -

BELL CANADA
BRAGG COMMUNICATIONS INC. dba EASTLINK
COGECO CONNEXION INC.
DISTRIBUTEL COMMUNICATIONS LIMITED
FIDO SOLUTIONS INC.
ROGERS COMMUNICATIONS CANADA INC.
SASKATCHEWAN TELECOMMUNICATIONS
SHAW COMMUNICATIONS INC.
TEKSAVYY SOLUTIONS INC.
TELUS COMMUNICATIONS INC.
VIDEOTRON LTD.

Third Party Respondents

- and -

SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC
BEANFIELD TECHNOLOGIES INC.

Intervenors

CONSOLIDATED PUBLIC REPORT

STATEMENT OF ISSUES

Four Key Issues:

1) **Review and verify** the application of the criteria by the Plaintiff's Agent for the identification of IP addresses for blocking, and provide the list of all IP addresses with dates and times on which they were required to be blocked (and criteria applied that resulted in them being notified for blocking);
2) **Compliance**- Gather facts regarding the Plaintiffs' and the Third Party Respondents' implementation of the Order (dated May 27, 2022 issued by the Honourable Justice Pentney), and the degree to which its specific terms are complied with, as well as any difficulties encountered by the Third Party Respondents;
3) **Compile Information** relating to any complaints received by the Plaintiffs or Third Party Respondents relating to the implementation of the Order; and
4) **Effectiveness Assessment** - Assessing the Order's effectiveness, including identifying the criteria for measuring success, explaining why these were selected and describing the results of this assessment.

INTRODUCTION AND SUMMARY

5) We want to begin by thanking the Third Party Respondents, the Plaintiffs, and the Plaintiffs' Agent for providing us with unfettered access to assist with carrying out the mandate of the Order, and for openly communicating with our team, and working efficiently to allow this Consolidated Public Report to be submitted to the Court in accordance with the terms requested in the Order.
6) Similarly to situations with other extraordinary relief granted previously by the Courts, including Anton Piller Orders, Mareva Injunctions and Norwich Orders, the forms and content of the initially granted orders following their implementation were amended over time as more information became available allowing the Court to satisfy itself that the implementation was done in the most efficient and respectful manner in consideration of all rights belonging to parties and non-parties. It is for this reason that, in many

instances, the Court has required an independent supervising solicitor (or expert) to oversee the implementation as an Officer of the Court.

7) We were able to review and independently verify the criteria used by FMTS to select IP addresses for inclusion in the blocklist.
8) Through the use of automation tools, 9 of 10 Third Party Respondents were able to block 100% of the IP addresses tested.
9) Notably, no legitimate complaints from any individual(s) or business(es) as it relates to the blocking.
10) In summary, we conclude that empirical data supports an assessment that the available supply of Infringing Copyrighted Content (to be defined) was reduced, and the Order has therefore met the necessary conditions for effectiveness, because it delivered that measurable benefit for a very low cost.

QUALIFICATIONS

11) David S. Lipkus is a partner at the Toronto, Ontario, law firm of Kestenberg Siegal Lipkus LLP. The principal focus of my practice is in the area of intellectual property.
12) David S. Lipkus received his Juris Doctor from the University Of Detroit Mercy School Of Law in 2008. David S. Lipkus received a BA in Honours Philosophy: Reasoning and Ethics in 2005 from The University of Western Ontario. David S. Lipkus became a member of the New York State Bar in March, 2009. David S. Lipkus was called to the Ontario Bar in January, 2010.
13) David S. Lipkus has conducted training sessions, workshops and lectures on intellectual property enforcement for various regional, municipal and Federal police forces, representatives of Canada Border Services Agency, private investigators, and various professional organizations.
14) David S. Lipkus has also regularly attended lectures, seminars and conferences on a variety of counterfeiting issues conducted by our firm and various intellectual property rights holders, including the International Anti-Counterfeiting Coalition (IACC), the largest international organization devoted solely to combating product counterfeiting and piracy and the International Trademark Association.

15) David S. Lipkus regularly reviews jurisprudential developments in the field of Anton Piller Orders, and is very much aware of the jurisprudence of this Honourable Court on Anton Piller Orders. David S. Lipkus is mindful of the importance of respecting the rights of the person(s) on which an Anton Piller Order is executed including third parties in attendance during the execution of an Anton Piller Order, and takes his responsibilities as an officer of the court in this regard very seriously.

16) David S. Lipkus has executed several Anton Piller Orders granted by this Honourable Court and the Superior Court of Justice in Ontario as an independent supervising solicitor.

17) David S. Lipkus' work as an independent supervising solicitor in the *Tracey Clancey et al v. Tanvir Farid* matter (file number CV-17-587516) was commented on by the Honourable Justice Pattillo at paragraph 36 of his endorsement:

> "I am satisfied, based on the material filed, that the APO was conducted in accordance with the terms of both the APO/Injunction Order and the December 11, 2017 Order extending it. I find that at all material times, the ISS and those accompanying him as authorized by the APO acted in both a courteous and professional manner at all times towards Farid."

18) On behalf of his clients, David S. Lipkus is involved with the removal of tens of thousands of online listings that include infringing content. David S. Lipkus has been provided with access to (and utilization of) numerous third-party provider software, to assist with these intellectual property takedowns efforts. Additionally, David S. Lipkus regularly reviews the policies of Registries, Registrars, ISPs, social media platforms, marketplaces and other intermediaries as it relates to intellectual property infringement.

19) Attached hereto and marked as Schedule A is a copy of David S. Lipkus's Curriculum Vitae including his rankings, speaking engagements, publications and memberships.

20) Jon Wilkins is a co-founder of Quadra Partners, LLC (Quadra), a strategic advisory firm providing business, public policy, and regulatory strategy in the telecommunications, media, and technology (TMT) sector.

21) Prior to founding Quadra in February 2017, Jon Wilkins spent over three years in leadership roles at the Federal Communications Commission (FCC). From March 2016 to

January 2017, Jon Wilkins was Chief of the FCC's Wireless Telecommunications Bureau. As the senior agency official with responsibility for the U.S. wireless industry, Jon Wilkins led a professional organization of over 150 lawyers, economists, and engineers. Jon Wilkins major policy activities included wireless spectrum, wireless infrastructure deployment, M&A transaction review, and competition oversight. In this role, Jon Wilkins had regular public speaking roles with respect to policy issues and engaged frequently with senior management of the United States telecommunications industry. Jon Wilkins was also responsible for a range of intergovernmental coordination activities including Congressional briefings and coordinating with the Department of Commerce and the U.S. Department of Defense on spectrum matters.

22) Prior to becoming Wireless Bureau Chief Jon Wilkins I was a Managing Director at the FCC. Having assumed this role in November 2013, Jon Wilkins served as the agency's chief operating official with authority over budget, personnel, information technology and cybersecurity, and federal contracting. Jon Wilkins also served as Advisor for Management to FCC Chairman Tom Wheeler and, in that capacity, Jon Wilkins worked with the Chairman's office and senior FCC staff on a number of strategic initiatives at the Commission. Most notably, Jon Wilkins led policy modernization efforts for the Universal Service Fund, which supports over $8 billion annually in advanced fixed and wireless telecommunications services.

23) Prior to joining the FCC in 2013, Jon Wilkins had spent 16 years at McKinsey & Company's Washington, DC office, where Jon Wilkins first became a partner in 2003. Jon Wilkins focus was on telecommunications matters, including the global Internet sector. Jon Wilkins firm consulted with most leading companies in the sector across all global geographies, which exposed Jon Wilkins to fundamental competitive concerns and business strategies of all of the providers. Jon Wilkins also served as a policy advisor in the Office of Plans and Policy at the FCC from 1998-1999, as a federal judicial law clerk from 1995-1996, and as a member of the Obama-Biden Presidential Transition Team in 2008-2009. Jon Wilkins graduated from Yale Law School in 1995 and Dartmouth College in 1992. Appendix A provides a copy of my Curriculum Vitae (CV).

24) Jeff Vansteenkiste is Manager of Internet Investigations at the Toronto, Ontario, law firm of Kestenberg Siegal Lipkus LLP, where he conducts online investigations in support of the intellectual property practices of the firm's lawyers. Mr. Vansteenkiste assisted as it related to all technical aspects in carrying out the mandate assigned by the Order.

25) He received a three-year diploma in Computer Security and Investigations from Fleming College in 2006 and a BA in Sociology from Trent University in 2010.

26) He has been employed as an investigator since 2010, providing digital forensics services and open source and undercover intelligence for employers and clients, largely in the realm of intellectual property investigation and enforcement. He is extremely familiar with internet technologies and architecture, online investigative techniques and best practices, as well as the online piracy landscape.

27) He was employed at Digital Evidence International in London, Ontario, from 2010 to 2014, where he primarily performed online investigations into piracy of satellite television content and digital software, as well as provided digital forensics services.

28) At the Motion Picture Association – Canada in Toronto, Ontario, from 2014 to 2015, Jeff conducted and coordinated a large number of online investigations into online movie and television piracy. Frequently, the subjects of his investigations were unauthorized online streaming websites and IPTV services.

29) From 2015 until the present, he has held a position as Manager of Internet Investigations at Kestenberg Siegal Lipkus LLP. The majority of his work concerns online investigation into the infringement of the firm's clients' intellectual property rights. He has performed extensive work for clients concerned with unauthorized IPTV devices and services, and conducted forensic examinations and network traffic analysis of said devices and services.

30) Jeff has acted as an expert in the service of Anton Piller Orders, both as a digital forensics specialist and for his knowledge of counterfeit products.

31) He has conducted training sessions, workshops, and lectures for multiple levels of law enforcement, legal professionals, various professional organizations, and private investigators on subjects such as online investigations, open and closed source

intelligence techniques, best practices, and analysis, digital forensics, as well as the identification of counterfeit products.

32) He also regularly attends lectures, seminars, and conferences on online investigations and open source intelligence techniques, best practices, and analysis. He continues to stay current on investigative techniques and issues through professional journals and print publications, blogs, and social networking.

DISCUSSION

Review and verify the application of the criteria by the Plaintiff's Agent for the identification of IP addresses for blocking:

33) The Plaintiffs' Agent (Friend MTS Limited ("**FMTS**")) searches for and identifies unauthorized copies of Copyrighted Content (as defined below) by using proprietary technology.

Review and Verification:

34) To facilitate our review and verification of the criteria for identifying IP addresses for blocking (including its application of the criteria set out in Confidential Schedule 2), FMTS provided us with a spreadsheet containing all IP addresses on the blocklist, and timestamps indicating when they were added to the blocklist, among other things. In total, 568 unique IP addresses were added to the blocklist.

35) When verifying these criteria, we used a sample set of 181 unique IP addresses (also tested during the live monitoring process as detailed below). The randomized selection of these unique IP addresses is detailed below in discussion of our live monitoring methodology.

Time Limits

36) Pursuant to the terms of the Order, IP addresses added to the blocklist are those determined by FMTS to be part of streaming infrastructure making the Copyrighted Content available without authorization during the NHL Live Game Windows, as well as during the Pre-Monitoring Period.

Verification:

37) Reviewing the blocklist, we confirmed that all 181 unique IP addresses were added to the blocklist during the NHL Live Game Windows, as well as during the Pre-Monitoring Period.

Proprietary Technology

38) FMTS uses proprietary technology which allows it to compare available content to legitimate samples of NHL games (referred to herein as "**Copyrighted Content**"). When matches are detected, the IP addresses of the source and associated streaming infrastructure are flagged for potential inclusion in the blocklist. Screenshots and video footage of the matched content are retained were made available, along with thumbnail images of the identified content and the legitimate sample content it was found to match.

Verification

39) To verify that the Copyrighted Content was properly identified, we reviewed all matches which resulted in an entry being made to the blocklist for the 181 IP addresses tested during our live monitoring process. Only blocklist entries added during the Pre-Monitoring Period, and NHL Live Game Windows for six games (Stanley Cup Finals games on June 15, 18, 20, 22, 24 and 26, 2022) were reviewed. Some of the 181 unique IP addresses were found to be associated with multiple matches throughout the Pre-Monitoring Period, and NHL Live Game Windows. In total, the selection included 356 blocklist entries associated with these 181 unique IP addresses.

40) Our validity checking involved visual review of thumbnail images, screenshots, and video captured from online video streams for each, and comparing them to reference images of the Copyrighted Content this streaming content was matched against.

41) We confirmed that 178 unique IP addresses were valid matches. The remaining 3 unique IP addresses unintentionally matched suspected pirated material, and FMTS immediately corrected the issue.

Determination of Absence of Legitimate Usage

42) FMTS indicated that not only does it use its knowledge of the online infringing video stream technologies to make a determination that a target IP address is unlikely to have any legitimate usage, it also uses technological methods. Only if all tests indicate there is no legitimate usage can it be added to the blocklist.

Verification

43) FMTS provided us with data on all such additional tests performed on potential target IP addresses. In reviewing this data, we confirmed that 80 unique IP addresses were associated with pirate streaming services, and were found by FMTS to pass all tests indicating there is no legitimate usage and the IP addresses can be added to the blocklist

Implementation

Live Monitoring

44) To assist with our monitoring of the Third Party Respondents' implementation of the Order, we were provided with access to their networks. With these connections, we were able to access the Internet through the Third Party Respondents networks in the same way their customers do. Additionally, FMTS provided us with the same level of access to the blocklist that the Third Party Respondents' have.

45) To monitor implementation, connectivity tests were performed through the Third Party Respondents' networks during six NHL Live Game Windows of the NHL Finals, beginning 30 minutes after the start of each. The date and times of these live broadcasts were:

- June 15, 2022, 8:00 PM EDT
- June 18, 2022, 8:00 PM EDT
- June 20, 2022, 8:00 PM EDT
- June 22, 2022. 8:00 PM EDT
- June 24, 2022. 8:00 PM EDT
- June 26, 2022. 8:00 PM EDT

46) These tests were used to determine whether IP addresses on the blocklist were accessible or had been successfully blocked on the networks. All Third Party Respondents had their implementation tested during at least three of the six games, although time restrictions and late provision of access to some of these networks meant we were unable to test all Third Party Respondents' implementation for every one of the NHL Live Game Windows.

Software Used

47) As it was highly unlikely that all hosts located at IP addresses on the blocklist were configured in the same way, three different software utilities were used to perform the connectivity tests, all of which generate different kinds of network traffic when in use. In this way we could be confident that a host configured to ignore the type of network traffic generated by one utility would not be erroneously marked as unreachable in our results.

48) Although some connectivity tests were manually performed, the majority of our testing was done using a software script we created which automates launching the utilities and saves their timestamped output. The timestamped output produced by the tools was provided to the Third Party Respondents and the Plaintiffs (and we have retained a copy).

49) The three chosen connectivity tests were Ping, Traceroute and Tcptraceroute, as follows:

Ping

50) The ping utility is one of the simplest computer networking utilities and was designed to measure round trip time for sending a packet to a remote IP address and receiving an acknowledgement packet in return. This measurement is often referred to as network latency. The ping utility is frequently used not to measure this network latency, but simply to determine if there is a live host located at the remote IP address.

Traceroute

51) Traceroute is used to trace the route traffic travels when communicating with a remote IP address. It attempts to enumerate every IP address the traffic passes through on its way to its destination and is often used to diagnose connectivity problems by identifying where a problem is occurring.

Tcptraceroute

52) Tcptraceroute performs the same function as the traceroute utility but uses different network packet types to do so.

Methodology

53) During each NHL Live Game Window, the process for performing connectivity testing on the Third Party Respondent's customer networks was as follows:
    a) Establish and verify a connection to the Internet through the Third Party Respondents' customer network;
    b) Launch the connectivity testing script;
    c) The script performs the following actions:
        i. Downloads and retains a current copy of the blocklist;
        ii. Randomly selects five IP addresses from this copy of the blocklist;
        iii. For each IP address selected, runs the ping, traceroute, and tcptraceroute utilities; and
        iv. Saves and timestamps all output from these utilities
54) The process was repeated for as many Third-Party Respondent networks as time permitted during each NHL Live Game Window.

55) It should be noted that, due to the limited time available during each NHL Live Game Window, these tests were configured to generate a very small amount of internet traffic in comparison to a typical user accessing streaming content. The technological methods some Third-Party Respondents used to implement the Order meant that our tests were sometimes able to reach blocklist IP addresses despite blocking being implemented properly on the tested network, as explained below. For this reason, a test which determined a blocklist IP address was reachable does not necessarily indicate non-compliance with the Order.

Results

56) Over the course of the live monitoring performed during the six NHL Live Game Windows, a total of 698 connectivity tests were performed on 181 unique IP addresses from the blocklist. Overall, 77.51% of these tests found that their target IP addresses

were unreachable by customers on the tested networks. Testing results for individual Third-Party Respondents consistently varied in accordance with their method of implementation. Overall, 9 of the 10 Third-Party Respondents had a 100% compliance rate.

57) A summary of the connectivity test results can be found in Table 1.

Log Data Review

58) Due to differences in infrastructure setup and size, internal organization, and technologies utilized, the order was implemented in different ways by the Third-Party Respondents. Using log data and other documentation provided to us by the Third Party Respondents, we compared implementation of the Order to our live monitoring testing results for the six NHL Live Game Windows of the NHL Finals. We have retained a copy of all documentation and information provided to us by the Third Party Respondents. In an effort to reduce the potential for over-blocking, some of the ISPs blocked the IP addresses after there was a certain threshold of network traffic. This is the reason for the differences in percentages between the live monitoring performed and the Log Data Review.

59) A summary of the Third-Party Respondents' implementation of the blocking can be found in Table 2.

Table 1– Connectivity Testing Results

	Overall
Tests	698
Reached IP Address	157
Did Not Reach IP Address	541
% Did Not Reach IP Address	77.51%

Table 2–IP Addresses For Which Blocking Was Implemented:

	ISP 1	**ISP 2**	**ISP 3**	**ISP 4**	**ISP 5**	**ISP 6**	**ISP 7**	**ISP 8**	**ISP 9**	**ISP 10**
Sample IP Addresses	181	181	181	181	181	181	181	181	181	181
Blocking Not Implemented	0	0	0	0	0	0	0	0	Unknown	0
Blocking Implemented	181	181	181	181	181	181	181	181	Unknown	181
% Blocking Implemented	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	Unknown	100.00%

Compile Information *relating to any complaints received by the Plaintiffs or Third Party Respondents relating to the implementation of the Order:*

E-mail Communications

60) As part of our mandate, we were provided with access to the T-955-21@proton.me email address (the contact information posted publicly for any inquiries or complaints related to issuance and implementation of the Order).

61) No legitimate complaints were received by the Plaintiffs. There was several vulgar emails from one individual that communicated displeasure with the issuance of the Order, generally. However, these were not relevant complaints.

62) Additionally, an email was received from an IPTV service advertising "free iptv sport, news, kids channel [sic]" along with a Whatsapp number and website address, and a second email relating to a spear phishing campaign.

Attached here and marked as Schedule C are copies of the redacted emails referred to herein (and we have retained an unredacted copy of the emails).

***FMTS*:**

63) FMTS received one relevant email, reproduced as follows:

"Sun, 17 Jul 2022 at 11:58 PM BST

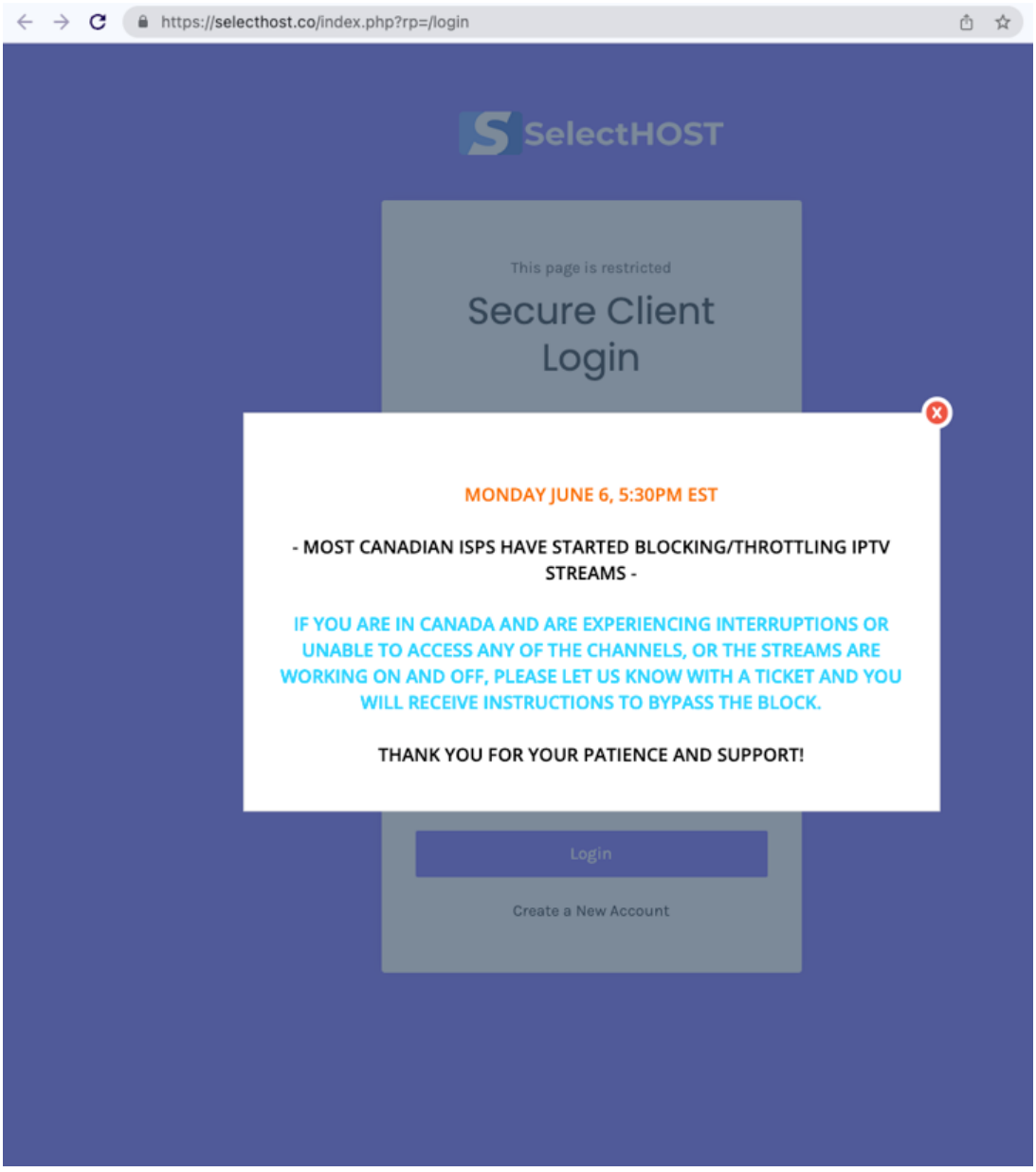
Hello I believe something in a order is blocking my access to non infringing content . Its a little annoying and interfearing with my rights as a consumer . I am not at all impressed , please look into this thank you.

[redacted]"

64) However, the timing of this email was after the blocking period, and despite a follow-up email from FMTS requesting additional further information, no specific details including

the IP address, the dates/times blocked, or any other details were provided, therefore this complaint is not likely genuine.

65) Additionally, after issuance of the Order, FMTS learned that a streamer of pirated content (SelectHOST) broadcasted a message to its customers (after logging into its service) warning its customers of potential access to channels/streams, and the availability of instructions to "bypass the block". A copy of the message referenced herein is reproduced below:



INTRODUCTION – EFFECTIVENESS ASSESSMENT

66) Further to Justice Pentney's Direction dated June 8, 2022, David S. Lipkus and Jon Wilkins jointly developed the criteria and explanation under this second mandate.

67) Effectiveness involves an assessment of how the Order impacted both the supply of and demand for Infringing Copyrighted Content online, including consideration of costs as well as benefits of reducing each.

68) The Court's mandate for an independent assessment of effectiveness of the Order does not seek a de novo analysis of dynamic site blocking in general as a policy matter. Instead, the mandate seeks an assessment of the effectiveness of the Order, and it provides a clear baseline of reference for the evaluation: the Court's finding that Plaintiffs "have established a very strong *prima facie* case that the unknown Defendants are engaging in ongoing breach of their copyright in the broadcasts of live NHL games [and] that the Plaintiffs will suffer irreparable harm if this is allowed to continue."[1]

69) Additionally, the Court found that the damage to the Plaintiffs from unauthorized streams of pirated material is "primarily financial" and although the evidence does not show with precision the financial value of the number of the Plaintiffs' lost subscribers, or of the decreased ability for the Plaintiffs to attract new customers due to the alternative of streaming of pirated material, the Court found that the NHL copyright piracy at issue in this case results in harm.[2]

70) Therefore, the approach to assessing effectiveness we will apply in this Report is to assess whether the Order resulted in reduced piracy and, as such, whether it delivered sufficient benefits to the Plaintiffs including in the form of reduced losses of subscribers to pirate services and/or additions of new subscribers so as to justify costs to third parties including ISPs and potential barriers[3] to Internet users in Canada.[4]

---

[1] *Rogers Media Inc. et al v. John Doe 1 et al* (2022 FC 775), at paragraph 9
[2] *Ibid* at paragraphs 164 and 165
[3] By "barriers" we refer to negative impacts on subscribers' ability to access non-infringing content that, although not directly experienced as financial costs, should be included in the overall weighing of costs and benefits to assess effectiveness.
[4] Any consideration of distributional effects, such as which parties should bear attendant costs required to realize available benefits, is beyond the scope of this Report.

71) Rights holders most likely benefit when blocking reduces the volume of actual Internet user consumption of Infringing Copyrighted Content, because – absent direct measurements – this provides the least speculative support for the inference that Court-mandated blocking effectively leads to an economic benefit to Rights Holders from increased use of legitimate material. Rights Holders may also benefit when blocking reduces the supply of Infringing Copyrighted Content, although, absent corroborating evidence of a resulting impact on consumption, such benefit is attenuated. To take the extreme illustrative example, blocking a site with Infringing Copyrighted Content that no Canadian Internet user ever seeks to access would have very little benefit to the Plaintiffs.

72) ISPs experience both direct costs for implementation as well as indirect costs due to the potential negative impact on customer experience, disruption to overall network management and customer service processes, and the uncertainty of how to prepare for future expansion of similar blocking requirements.[5]

73) Internet Users potentially experience barriers primarily in the form of "over-blocking," including loss of access to legitimate material as well as loss of access to "otherwise unauthorized" material that may infringe the rights of certain rights holders (other than Plaintiffs). Although not as easily quantified as the costs to ISPs, the potential negative consequence of losing access to non-infringing material for Internet users should also be considered in an overall cost-benefit assessment of effectiveness.

Elements of Effectiveness

74) There are four main elements of effectiveness to address in this Report, as follows:

a. Effectiveness as it relates to the benefits to Rights Holders in reducing the consumption of infringing material. Specifically, this includes reducing the use of infringing live NHL game footage ("**Infringing Copyrighted Content**"), including future use, and potentially

[5] Note that this assessment may vary between independent ISPs and "tied" ISPs, which operate within larger corporate enterprises that also capture the benefits of blocking that accrue to Rights Holders.

increasing the use of the Rights Holders' legitimate services. "[Piracy] is among the reasons that people are either choosing to stop their subscriptions or not signing up in the first place"[6]. Determining whether the Order was effective includes learning whether it will "discourage Internet users from accessing the infringing service[s]," including consideration of the overlapping issues of "dissuasiveness and substitution"[7] as "it has been recognized that adding costs to the unauthorized streaming may bring the user's total costs of accessing infringing material closer to the costs of legal subscription"[8];

b. Effectiveness as it relates to the benefits to Rights Holders with respect to reducing the supply of Infringing Copyrighted Content. Specifically, this includes determining whether the Order "will make infringing activities more difficult to achieve"[9];

c. Effectiveness as it relates to the costs borne by the ISPs with respect to implementing the blocking in the Order: "The factors to be considered [include] … whether alternative and less onerous measures are available[,]complexity and cost"[10]; and

d. Effectiveness as it relates to the potential barriers to Internet users due to over-blocking: "whether the relief will ... unduly affect[] the ability of users ... to access information lawfully"[11].

75) Therefore, our joint proposed definition of Effectiveness: "Did the Order measurably result in sufficient benefits to the Plaintiffs to be worth the cost to ISPs and potential barriers to Internet users?"

[6] *Rogers Media Inc. et al v. John Doe 1 et al* (2022 FC 775), at paragraph 165
[7] *Ibid* at paragraph 224
[8] *Ibid* at paragraph 237
[9] *Ibid* at paragraph 224
[10] *Ibid* at paragraph 113
[11] *Ibid* at paragraph 245

CRITERIA FOR MEASURING SUCCESS

Proposed Criterion 1: Benefits with respect to demand for Infringing Copyrighted Content:

76) To what extent did the implementation of the Order prevent or deter Internet users in Canada from accessing the Infringing Copyrighted Content?

Basis for Proposed Criterion 1

77) Even if the dynamic site blocking process successfully blocked the supply of a certain amount of Infringing Copyrighted Content, a robust assessment of effectiveness must evaluate whether users were actually accessing those sites (i.e., consumption of infringing material would have occurred but for the blocking), whether users easily located alternative sources non-blocked infringing material, and/or if some users were in fact discouraged or dissuaded from continuing to seek infringing material.

Preferred Metrics:

78) For each blocked IP address, how many unique user requests for access to that IP address were blocked during each NHL Live Game Window?

79) For each blocked IP address, how did the volume of Internet user requests during the NHL Live Game Window compare to a baseline volume of requests to the same IP address outside of NHL Live Game Window periods? In other words, did the volume of Internet user requests to the blocked IP address increase during the NHL Live Game Windows?

80) What variation in demand volume was seen across the blocked IP addresses during each NHL Live Game Window? For example, what percentage of the blocked IP addresses made up 80% of demand volume for the total blocklist over the entire duration of each Window?

81) What variation in demand was seen across the NHL Live Game Windows for IP addresses that were included in the blocklist for multiple games?

82) What demand was there for IP addresses identified to have Infringing Copyrighted Content but not included in the blocklist? Did this demand and/or consumption increase after the implementation of the Order?

Available Metrics

83) During the live game monitoring, a number of ISPs tracked partial demand data.

84) One ISP provided data on the number of unique customer IP addresses that attempted to access IP addresses on the blocklist during each NHL Live Game Windows during which the Order was in place. However, the system used to log this data is only capable of recording a maximum of 300 unique customer IP addresses per NHL Live Game Window and the ISP was unable to provide total numbers for the period the Order was in effect. The recorded numbers for individual NHL Live Game Windows ranged from 109 to the maximum of 300. The logging system reached this maximum limit for the first time on June 5, 2022, and did so during every NHL Live Game Window thereafter.

85) Although unable to enumerate unique customer IP addresses attempting to access IP addresses on the blocklist, one ISP was able to provide log data showing dropped Internet traffic toward blocklist IP addresses during the NHL Live Game Windows. This data indicated 5,613,142 packets bound for 21 separate blocklist IP addresses had been dropped by the ISP's implementation of the blocking. We note that lacking any other context with respect to the nature of this traffic, it is not possible to draw any meaningful inferences from this information.

86) One ISP indicated that a total of 40,105 unique customer IP addresses attempted to access IP addresses on the blocklist during the NHL Live Game Windows.

87) One ISP delayed implementation of the blocking until 15-25 minutes into each NHL Live Game Window. This ISP was able to collect data on the number of unique customer IP addresses that attempted to access IP addresses on the blocklist during the 30-60 minutes prior to each NHL

Live Game Window and during this brief period before blocking began. It was unable to track this traffic while the blocking was in place, but during the period it was able to collect data, a total of 50,794 unique customer IP addresses were found to have attempted access to IP addresses on the blocklist. Numbers for individual games ranged from 2,663 to 11,236 unique customer IP addresses.

88) One ISP was able to implement limited logging of unique customer IP addresses attempting to access IP addresses on the blocklist during the final four NHL Live Game Windows during which the Order was in place. This number ranged from 848 to 971. It should be noted that this ISP was implementing the blocklist through a manual process and only able to block 200 IP addresses from the blocklist per NHL Live Game Window, and therefore had no ability to track traffic to IP addresses for which it was unable to implement blocking.

89) This data is directionally useful for demonstrating that at least a sub-set of the IP addresses included in the blocklist were associated with user demand during the NHL Live Game Windows. It is clear that the IP addresses included in the blocklist in aggregate were relevant to Canadian users during the NHL Live Game Window. It is possible that some of the demand was for content other than Infringing Copyrighted Content, because we do not have data for other content that may have been available on these IP addresses.

90) However, data was not available for the following metrics:

a. Changes in demand for a given IP address before/after/during the NHL Live Game Window. Increases in demand during NHL Live Game Windows would be a more reliable indicator that the site was in fact serving as a destination for users seeking infringing content.

b. Distributional data on relative demand for different sites within the overall set of IP addresses included in the blocklist.

c. Information about demand for IP addresses not included in the blocklist known to contain Infringing Copyrighted Content (i.e., sites identified via proprietary technology to contain infringing NHL material but not meeting the criteria for being added to the blocklist).

Conclusion - Proposed Criterion 1 (Benefits with respect to demand for Infringing Copyrighted Content):

91) Overall, the Order was effective in reducing access to the Infringing Copyrighted Content for at least tens of thousands of Internet users in Canada. However, it is not possible based on the data provided to draw reasonable conclusions about Canadian Internet user behavior with respect to demand for the Infringing Copyrighted Content or what steps may have been taken by Internet users in Canada while the IP addresses were being blocked by the ISPs. The facts we do know are that at least 92,170 Internet users in Canada were likely blocked initially when they attempted to access the blocked IP addresses (although we do not have data confirming that these users were seeking live NHL game footage on these addresses versus other content that may have been available), and at least one pirate network attempted to assist Internet users in Canada in circumventing the Order[12]. However, without access to additional data (for example, whether those users were easily able to access other unauthorized streams, the number of subscribers gained following implementation of the Order, and/or the number of new users attempting to access the legitimate streams) it is difficult to draw any further conclusion with respect to whether the Order effectively reduced demand for the Infringing Copyrighted Content in such a way that would benefit the financial interests of Plaintiffs, especially in light of the limited timeline associated with this mandate.

92) We note that any data available as it relates to Internet user behavior after blocking was implemented, and whether this discouraged or dissuaded Internet users from accessing the infringing material would be highly relevant (including, for example, if an Internet user's IP address later resulted in (1) a new legitimate subscriber, or (2) an attempt to access the legitimate streams available in Canada).

Proposed Criterion 2: Benefits with respect to reduced supply of Infringing Copyrighted Content:

93) To what extent did the implementation of the Order reduce the availability of Infringing Copyrighted Content during the NHL Live Game Windows?

[12] See Consolidated Public Report, paragraph 65

Basis for Proposed Criterion 2

94) To be said to be even potentially effective, the dynamic blocking scheme must be shown to have had at least a measurable impact on the availability of infringing material; to be said to be actually effective, such impact should be shown to have had a material impact sufficient to impact the economic choices of Canadian Internet users as between pirate services and legitimate services.

Preferred metrics:

95) Reproduction of Infringing Copyrighted Content: Did the specified IP addresses reproduce Infringing Copyrighted Content during the NHL Live Game Windows (and/or immediately prior to them) that, but for the dynamic blocking, would have been available to Canadian Internet users? How many did / did not?

96) Changes over time: What changes occurred in the designated list of addresses during the duration of the dynamic blocking process? What changes during a given NHL Live Game Window (hourly refreshes)? What changes across the various NHL Live Game Windows? Did these metrics or other factors support the conclusion that pirate services were altering their behavior in response to the Order, thereby supporting an inference that blocking at least some of the IP addresses was having a measurable effect?

97) Assessing whether impact is material. Did the blocked IP addresses represent a material impact on the availability of Infringing Copyrighted Content, based on information from FMTS regarding the total size of the supply of such material during the implementation of the Order, similar to the monitoring conducted between January 30, 2021 – May 30, 2021? Additionally, are there alternative sources or factual bases for assessing whether the blocked IP addresses represented a de minimis, material, or substantial portion of the supply of Infringing Copyrighted Content (for example, by reviewing open source intelligence including search engines, sites, message boards, social media and other various data regarding the availability of pirated streams in Canada including Infringing Copyrighted Content)?

Available Metrics

98) The implementation of the Order by the ISPs did reduce the availability of Infringing Copyrighted Content. Independent monitoring verified that almost all blocked IP addresses contained at least some reproduction of Copyrighted Content, and 9 of the 10 ISPs successfully blocked access to these sites for almost all of the NHL Live Game Windows.[13]

99) Given the limited duration of the implementation of the Order and without more data on the overall number of available Internet sites reproducing Infringing Copyrighted Content in Canada (i.e., including those that did not meet the Court's criteria), it is especially difficult to determine the impact on the overall supply of Copyrighted Content. It is of course not required that all or even most Infringing Copyrighted Content be blocked to have a material impact.

Conclusion - Proposed Criterion 2 (Benefits with respect to reduced supply of Infringing Copyrighted Content)

100) As a result of the Order, a blocklist included 568 unique IP addresses including Infringing Copyrighted Content that were inaccessible by Internet users in Canada[14] and there is no debate that this reduced the available supply of Infringing Copyrighted Content. An "effective" impact on the supply of Infringing Copyrighted Content would be enough to be "noticed" by Internet users seeking such material, causing some impact on their ability to access such material and therefore giving rise to a reasonable inference of some potential benefit to Plaintiffs' ability to attract at least some Canadian Internet users to legitimate services. The limited duration and monitoring record available here does not allow us to make any further conclusions as to effectiveness on this criterion.

Proposed Criterion 3: Potential barriers with respect to the supply of non-infringing material ("over-blocking"):

[13] See Initial Confidential Report of David S. Lipkus, paragraph 65 and Table 3
[14] We do note that one ISP was not able to fully implement the blocking. See Initial Confidential Report of David S. Lipkus, paragraph 73

101) To what extent did the Order reduce the availability of non-infringing material found on servers subject to blocking during the NHL Live Game Window? To what extent did the dynamic blocking process negatively impact legitimate activity by Internet users in Canada?

Basis for Proposed Criterion 3

102) A reasonable definition of effectiveness must balance the benefits to Rights Holders of reducing the availability of infringing material versus the potential harm to Canadian Internet users of reducing the availability of non-infringing material.

Preferred metrics:

103) How many blocked sites provided access to material other than Infringing Copyrighted Content? What mix of "otherwise unauthorized" versus legitimate content versus Infringing Copyrighted Content?

104) How many blocked IP addresses contained legitimate material?

105) What Internet user complaints related to over-blocking were received?

106) What variation in demand volume was observed across specified IP addresses, including based on relative amount of Infringing Copyrighted Content versus non-infringing material?

107) How did the volume of requests during NHL Live Game Windows compare to a baseline volume of requests to the same IP addresses outside of the NHL Live Game Window?

Available Metrics

108) As noted by the Court, the measures used to implement the Order err on the side of under-blocking.[15]

109) No ISP reported any legitimate Canadian Internet user's complaints related to lost access to legitimate material, nor were any legitimate complaints received by the Plaintiffs and FMTS.[16] Further, from our review of the Federal Court Recorded Entries, no third party brought an application to the Court attempting to vary or discharge the Order.

Conclusion - Proposed Criterion 3: Potential barriers with respect to the supply of non-infringing material ("over-blocking"):

110) On balance, given the particularly targeted nature of the criteria for blocking in this case, we do conclude that the Order was effective at limiting over-blocking of truly legitimate material.

Proposed Criterion 4: Operational effectiveness of the dynamic blocking in this case:

111) Based on the findings of the Initial Confidential Report, how operationally effective was the implementation of the Order?

Basis for Proposed Criterion 4:

112) Operational feasibility of implementation is a prerequisite to any assessment of effectiveness.

[15] *Rogers Media Inc. et al v. John Doe 1 et al* (2022 FC 775), at paragraph 177
[16] See Consolidated Public Report, paragraphs 60-64

Evaluated Metrics (per the Order):

113) Proper application of the criteria for the identification of IP addresses for blocking and verification of underlying justification as reflected in data provided by FMTS and consistency with the Confidential Schedule 2 criteria.

114) Compliance by ISPs with implementation requirements of the Order and verification via live monitoring testing of randomly selected IP addresses during NHL Live Game Windows, and/or post facto log review/other documentation provided by ISPs.

115) Complaints received by either ISPs or Internet users, including the operational complexity/associated costs of implementation by the ISPs.

Conclusion - Proposed Criterion 4: Operational Effectiveness/Core findings of the Initial Confidential Report:

116) FMTS did appropriately apply the criteria to identify IP addresses for blocking. 178 out of 181 tested IP addresses were independently verified to meet the Order's criteria. As stated earlier, the 3 remaining IP addresses included suspected pirated content.

117) No material complaints were received, including no reports of excessive operational burdens or costs by ISPs to implement the Order (notably considering the Order's limited mandate with respect to requiring material changes to ISP systems and practices).[17]

Assessment of effectiveness based on measured criteria

118) The Order adopted an approach of directly targeting the supply of Infringing Copyrighted Content (i.e., blocking specified IP addresses) in order to have an impact on the demand for, and hence consumption of, Infringing Copyrighted Content (protecting the economic interests of

[17] We suggest the use of an automated system to implement the blocking is the preferred approach. See Initial Confidential Report of David S. Lipkus, paragraph 73

Rights Holders). As discussed in the Initial Confidential Report, for the most part the Order was successfully implemented.

119) We believe that the costs to ISPs were very low, largely due to the flexibility provided by the Order that in effect did not require any material change to existing ISP systems or operations.

120) The dynamic site blocking approach had a measurable beneficial impact on the availability (supply) of at least some Infringing Copyrighted Content during the NHL Live Game Windows, with a total of 178 unique IP addresses verified to have Infringing Copyrighted Content effectively blocked during the implementation of the Order, a very high percentage of a representative sample of the 568 unique IP addresses subject to blocking.

121) There were no measurable barriers to Canadian Internet users from over-blocking of fully legitimate material. We note that an unknown amount of "other unauthorized" material was blocked, and the impact on the Court's assessment of effectiveness as it relates to this issue was not reviewed.

122) We lack sufficient data to reliably assess the overall materiality of the Order on reducing the total supply of Infringing Copyrighted Content. Lacking additional measurement of (any of): (1) Infringing Copyrighted Content that would have been available on IP addresses not included in the blocklist, including any shifts in such supply in response to the implementation of the Order; (2) Infringing Copyrighted Content via IP addresses not on the blocklist; or (3) Infringing Copyrighted Content from non-monitored sources – it is not possible to further assess the overall materiality of the Order's impact on the supply of Infringing Copyrighted Content during the implementation period.

123) To be precise, lacking any of this broader context with respect to the supply and demand of Infringing Copyrighted Content, and changes to Canadian Internet user behavior following implementation of the Order, we cannot reach any further inferences as to whether the dynamic blocking approach here had any effect on the economic harm caused to the Plaintiffs. We do believe that, over time, the Plaintiffs may be in a better position based on available data (such as new subscribers or available streaming figures) to help supplement the record regarding the economic harms it suffered.

Conclusion: Overall assessment of effectiveness

124) Overall, we conclude that the Order as implemented did have a measurable effect on reducing the supply of Infringing Copyrighted Content, that over-blocking of legitimate material to Canadian Internet users was likely not a barrier, and that the Order proved implementable by all but one of the ISPs within the cost-limiting constraints imposed by the Court. The Order therefore did result in some degree of benefit for very low cost, and so can be said to have been effective.

125) We note due to the limited data available that we cannot more broadly assess the Order's effectiveness on a cost-benefit basis, or the implications for future scenarios involving longer duration, volume and complexity of dynamic blocking, and potentially higher costs for affected ISPs.

i. First, although with respect to supply, a number of sites containing Infringing Copyrighted Content were effectively blocked, we lack empirical data to make any reasonable inferences with respect to the impact on the overall supply of Infringing Copyrighted Content (in terms of impact on the economic harm to Plaintiffs).

ii. Second, with respect to actual Canadian Internet user demand behavior (deterring and dissuading use of Infringing Copyrighted Content), we lack empirical data to make any reasonable inferences with respect to whether, even for those Internet users who may have attempted to access to a given site, the dynamic blocking approach here had any impact on the economic interests of Plaintiffs.

126) In summary, we conclude that empirical data supports an assessment that overall supply of Infringing Copyrighted Content was reduced, and the Order has met the necessary conditions for effectiveness, because it delivered that measurable benefit for what we believe to be a low cost.

127) We note that this conclusion with respect to the Order in this case includes the consideration that there was a low cost of ISP implementation given the limited scope of the mandate (only one game per night for 6 nights), and the Court's cost-limiting flexibility granted to the implementing ISPs. We were able to verify reduced access to Infringing Copyrighted

Content to at least 92,170 Internet users in Canada, but were unable to verify most other potential areas of benefit.

128) Below, we include a list of considerations to establish whether implementation was effective that were not assessed within the scope of the Initial Confidential Report:

i. Verification of FMTS determinations with respect to the criteria used to select sites for blocking:

i.1 - Identification of IP addresses excluded from Confidential Schedule 2.

i.2 – Verification of "other unauthorized material" versus "legitimate" material:

- Although FMTS performs testing on IP addresses, more comprehensive testing, such as a full port scan, may enumerate what additional services, if any, are being hosted on these IP addresses.

ii. An expanded approach to live monitoring that is able to capture a larger number of blocked IP addresses and that is compatible with all automated blocking methods used by ISPs:

ii.1 - Live monitoring that is able to test more than just a small sample of blocked IP addresses, and/or is able to test a sample of a much larger number of blocked IP addresses.

ii.2 - Live monitoring that can be implemented for ISP blocking methods based on "traffic sensitive" methodology, rather than relying only on after-the-fact log review method.

iii. Capturing monitoring data about Internet user activity with respect to blocked sites:

iii.1 - As part of this monitoring effort, a number of ISPs were able to capture partial data about Internet users attempts to access blocked sites and this data provides useful independent validation that the criteria used to identify blocked sites in fact results in effective targeting of sites with Infringing Copyrighted Content that were the subject of at least some end-user demand during the Live Game Windows, even though we cannot independently confirm how many of these users were actually seeking access to Infringing Copyrighted Content versus other non-infringing material that may have been available via those sites.

iii.3 - The most useful information would be comparisons of demand for blocked sites both outside and inside NHL Live Game Windows.

129) A more complete assessment of effectiveness could include additional measurement and analysis, including one or more of the following:

iii. Developing a more thorough record on the scalability of implementation costs to ISPs as volume and frequency of required blocking grows. For example, what would be the costs to ISPs of doing this for 10 games per day over a 6-month season? Can all ISPs automate their processes? What resources are required? Are costs of broader implementation different as between tied versus independent ISPs?

iv. Without breaching any privacy obligations, conducting a quantitative analysis of how blocking impacts user behavior over a longer period of time, such as by sampling a statistically significant number of randomly selected, properly anonymized sets of unique end-user IP addresses on a regular basis to assess what video streaming sources (both Copyrighted Content and non-infringing content) are accessed and when. Measuring changes in observed streaming consumption behavior over a longer time involving periods of both active blocking (e.g., during NHL Live Game Windows) and no blocking may provide a reliable empirical basis for drawing conclusions about the actual benefits to Rights Holders.

v. Assessing whether the total volume of blocked sites must grow to address pirate efforts to evade blocking, especially for dynamic blocking approaches implemented for longer time frames (such as an entire NHL season).

vi. Measuring the effect of blocking on paid subscriptions or legitimate service viewership or subscription levels (this might require a long period of time to be measured, such as an entire regular season and playoffs).

vii. Conduct longer and broader monitoring to develop a factual assessment of the overall universe of Infringing Copyrighted Content to help determine likely effectiveness of blocking at reducing supply in a material way that will matter to Internet users.

130) Finally, we note that the assessment approach described in paragraphs 128-129 would require coordination between ISPs, and especially between tied and independent ISPs. A given tied ISP for example would be able to measure each of the listed factors within the scope of its regular business activities if it took the additional step of retaining FMTS or a similar firm to monitor changes in the supply of available infringing content. An independent ISP, however, would not have direct access to information about user behavior with respect to the legitimate sources of material. Admittedly, we are not aware of the costs to both the tied ISPs and independent ISPs associated with this type of assessment.

Jon Wilkins

David S. Lipkus