Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users

Shane Alcock
University of Waikato
Hamilton, New Zealand
salcock@cs.waikato.ac.nz

Richard Nelson
University of Waikato
Hamilton, New Zealand
richardn@cs.waikato.ac.nz

ABSTRACT

The Copyright (Infringing File Sharing) Amendment Act 2011 (CAA) is a New Zealand law that aims to provide copyright holders with legal recourse when content is illegally shared over the Internet. This paper presents a study of residential DSL user behaviour using packet traces captured at a New Zealand ISP before, shortly after and several months after the CAA coming into effect. We use libprotoident to classify the observed traffic based on the application protocol being used to identify and examine any changes in traffic patterns that may be a result of the new law. We find that the use of peer-to-peer applications declined significantly once the CAA was in effect, suggesting a strong correlation. We also found that there were increases in tunneling, secure file transfer and remote access traffic amongst a small segment of the user population, which may indicate an increased uptake in the use of foreign seedboxes to bypass the jurisdiction of the CAA.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations

Keywords

P2P, seedbox, traffic classification, residential DSL, Internet law

1. INTRODUCTION

The use of Internet file sharing technologies for copyright infringement has received significant attention from lawmakers in many countries. France, South Korea and the United Kingdom were among the first to enact legislation allowing for a graduated response to copyright infringement on the Internet. These countries employ a "three-strikes" approach where the offender receives warnings for the first and second infringements but may have their Internet connection terminated if infringing continues.

IMC'12, November 14–16, 2012, Boston, Massachusetts, USA.

On the first of September 2011, New Zealand joined these countries with the Copyright (Infringing File Sharing) Amendment Act [15] (which we shall henceforth refer to as the CAA). The CAA implements a graduated response system whereby copyright owners can advise the user's ISP when they believe a subscriber has breached copyright. The copyright holder must pay a NZ $25 processing fee (approximately $20 US) to the ISP and the ISP in turn must then issue an infringement notice to the suspected party. After three infringements, the subscriber can be taken to the New Zealand Copyright Tribunal by the copyright holder where the subscriber can be fined up to NZ$15,000. The law also has a (currently inactive) provision for the termination of an offending subscriber's Internet connection.

The CAA received widespread media coverage both inside and outside of New Zealand and the vast majority of New Zealand Internet users will have been aware of the new law by the time it came into effect. However, media reports differed as to whether the law was having any impact on user behaviour, i.e. whether users had ceased file sharing. One major New Zealand ISP reported a 10% decrease in peer-to-peer (P2P) traffic, another stated that international traffic had declined but was unable to determine whether this was related to file sharing while a third claimed there had been no discernible impact on traffic volumes [18]. None of the three ISPs provided any detail as to the measurement approach used to reach the publicised conclusions.

Therefore, we have conducted an investigation into the application protocols used by residential DSL users in New Zealand, both prior and subsequent to the CAA coming into force, to analyse the effect of the CAA on the behaviour of Internet users. We have analysed packet traces captured from a single New Zealand ISP using libprotoident [19], a traffic classification library and compared the popularity of different applications (e.g., P2P, web, mail) both before and after the CAA came into effect.

Unlike earlier studies that have looked at the impact of similar laws in other countries, such as [9] and [10], our study is based on measurements of the traffic sent and received by a cross-section of Internet users. Using this approach, we can easily and effectively analyse the behaviour of a large group of Internet users in an objective fashion.

Our results show that P2P traffic had more than halved by the time the CAA became an active law, suggesting that there may be a strong correlation between anti-file-sharing legislation and the use of P2P applications. Traffic volumes also declined notably for newsgroups and encrypted transfers. By contrast, we observed that protocols which can be

used as secure or private mechanisms for direct file transfers had become much more popular than they were prior to September 2011. These results suggest that, while the CAA may have had the intended effect of discouraging New Zealanders from partaking in P2P file sharing, some users have simply changed their approach to acquiring copyrighted material to avoid detection by rights-holders.

It should be noted that, due to the difficulties in obtaining suitable packet traces, this study has examined only a small portion of New Zealand Internet traffic and therefore we cannot irrefutably prove that the decline in P2P traffic has been caused by the new law. There are other possible reasons for the changes that we observed that cannot be ruled out with the data that we have: for example, a global trend in declining P2P traffic [12]. Therefore, the results of this study should be seen as an observation of a strong correlation that we believe is both interesting to the Internet research community and deserving of more detailed analysis in the future.

2. RELATED WORK

Other studies have examined the impact of laws similar to the CAA enacted in other countries. Dejean [10] surveyed a group of Internet users in Brittany following the enactment of the HADOPI law in France. They found that 25% of users had altered their downloading habits but less than 15% had ceased using peer-to-peer file sharing entirely. Many of those that had stopped using peer-to-peer had moved to alternative forms of file sharing, such as illegal streaming. Danaher [9] attempted to correlate the introduction of HADOPI with changes in online sales statistics for music. This study also suggested that HADOPI had a measurable impact, as song and album sales had increased significantly compared with other countries without similar legal ramifications for downloading copyrighted material.

Unlike the aforementioned research, we use Internet traffic classification techniques to conduct our study. Traffic classification has been a popular area of research over the past decade, especially with regard to identifying and analysing peer-to-peer traffic. The current state of the field has been well documented by several summary papers [7] [8] [16]. We used the libprotoident library [19] to classify the measured traffic for our study. Libprotoident is a lightweight payload inspection tool which uses only a small amount of application payload to identify the application protocol. This approach is similar to that used by Aceto et al. [3] with the PortLoad software but, unlike libprotoident, PortLoad is not publicly available nor has it been used to conduct any studies similar to this one.

With regard to identifying and measuring peer-to-peer traffic, Perényi [17] proposed a set of heuristics for identifying P2P traffic from NetFlow records. This technique was used to analyse the characteristics of P2P traffic observed at a Hungarian ISP, although they were only able to identify individual applications in cases where the default port was used. Another example is Hu [11] which developed behavioural profiles which could identify BitTorrent and PPLive traffic with high accuracy. There have also been studies using statistical and machine learning techniques to identify Internet applications [6] [13] [14]. These offer promising results but do not offer enough confirmed reliability for the analysis we intended to conduct, particularly with regard to identifying P2P traffic.

	Jan 2011	Sept 2011	Jan 2012
Start Date	06 Jan	12 Sept	16 Jan
Duration	7 days	8 days	8 days
Incoming Bytes	5,159 GB	5,079 GB	5,459 GB
Outgoing Bytes	919 GB	790 GB	896 GB
Active Subscribers	4928	4333	4135

Table 1: The trace sets used in this study. Incoming and outgoing bytes refer to the DSL network only. Active subscribers refers to unique IP addresses owned by the ISP that transmitted at least one packet.

3. METHODOLOGY

3.1 Data Sources

Packet traces that were captured using a passive monitor placed within the core network of a New Zealand ISP were used for this study. Although not large by New Zealand standards, the ISP offers DSL plans that are comparable in price, speed and data allowance with most competing ISPs in the New Zealand broadband market. The ISP operates on a nationwide basis and attracts customers from throughout the country, so we believe that the data set should be sufficiently representative for the purposes of our study.

The monitor was able to capture all bidirectional traffic for a subset of the ISP customer base. Each trace set was captured using an Endace DAG 4.3GE hardware capture card [2] and was entirely contiguous; all packets passing through the passive monitor between the start and end of the capture were written to disk. The trace sets are described in more detail in Table 1.

The timing of the captures was important for this study. The traces cover three distinct time periods: one week in January 2011, eight days in September 2011 and eight days in January 2012. The CAA came into effect on September 1, 2011. The January 2011 capture will therefore provide a suitable indication of user behaviour before the subscribers became conscious of the CAA. The September 2011 capture will demonstrate what, if any, immediate impact the new law may have had on user behaviour. Finally, the January 2012 capture will enable us to look at the possible effects of the CAA in the medium term and compare the traffic pattern with a similar time period from the previous year [1].

During the capture process, each packet was truncated to only contain the headers up to and including the transport header, i.e. the TCP or UDP header, plus an additional four bytes of application payload. The extra payload (captured with the permission of the ISP) allowed us to use libprotoident to classify the traffic, while minimising the potential impact on the privacy of the network users.

When performing the analysis, we used IP ranges provided by the technicians at the ISP to filter the captured traffic to only include traffic involving residential DSL subscribers. We chose to focus on residential DSL only as this user type was the principal intended target of the CAA. However, we will consider examining the effect of the CAA on other user classes, e.g. corporate Ethernet, in future work.

[1]Being different months, January and September may have had different traffic patterns for non-legislative reasons.

Category	Example Protocols
Chat	IRC, MSN, XMPP, Yahoo
Encryption	Unclassified SSL/TLS
Files	FTP, Rsync, SMB, Orbit
Gaming	Steam, Gamespy, XboxLive, WoW
Mail	SMTP, POP3, IMAP, IMAPS
NAT Traversal	STUN
News	NNTP
P2P	BitTorrent, Gnutella, EMule Pando, Manolito
P2P Structure	BitTorrent UDP, Gnutella UDP Emule UDP, Pando UDP
P2P TV	PPStream, PPLive
Remote	SSH, RDP, Teamviewer
Services	DNS, NTP
Streaming	RTMP, RTSP, Flash, Realplayer
Tunneling	TOR, OpenVPN, Teredo, ESP
VOIP	Skype, SIP, RTP, Teamspeak
Web	HTTP (incl. YouTube), HTTPS

Table 2: Categories supported by Libprotoident.

3.2 Analysis

We developed a program to read and analyse the packet traces using libtrace [4] and libprotoident [19]. Libtrace is a trace processing library that supports multiple capture formats and is required by libprotoident. Libprotoident is a traffic classification library that attempts to identify the application protocol being used by each flow observed in a packet trace using a technique known as lightweight packet inspection. Unlike deep packet inspection software, libprotoident only requires four bytes of application payload to be present in each captured packet. The version of libprotoident that we used, 2.0.5, supported over 200 unique application protocols including twelve P2P protocols and has been shown to achieve better accuracy than existing open-source deep packet inspection software [5].

The analysis program examined each flow that started and ended within the period covered by each trace set and reported the number of bytes downloaded, byte uploaded and active subscribers observed for each application protocol. Because the three data sets have different durations, the analysis and comparison of traffic volumes has been based on the mean amount of traffic observed per day rather than the total amount of traffic observed.

Each application protocol supported by libprotoident was also assigned to a category which described the purpose of the protocol, such as Web, P2P or Mail. The categories that were most prominent in our data sets are described in Table 2. In this paper, we present some results at the category level, as this can provide a clearer view of general user behaviour than examining popular individual applications.

One useful feature of our data set is that, unlike some DSL providers, the ISP that we have monitored assigned static IP addresses to DSL subscribers. We use the term subscriber to refer to a single premise that is being provided with broadband by the ISP. There may be multiple users associated with a single subscription; for example, residents of the same house who are sharing a broadband connection. We have assumed that a local IP address in a given trace set always corresponded to the same subscriber for the duration of the capture. This allowed us to investigate the number of subscribers using each application protocol or category over the course of each trace set. However, given the likelihood of customer churn over the course of several months, we did not extend this assumption across trace sets.

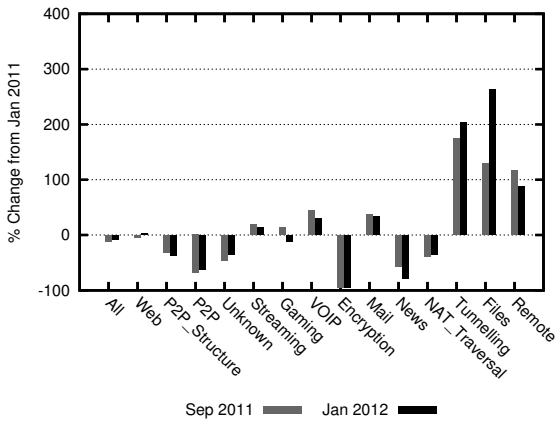

Figure 1: Bytes downloaded by residential DSL subscribers relative to the value observed in January 2011, broken down by application category.

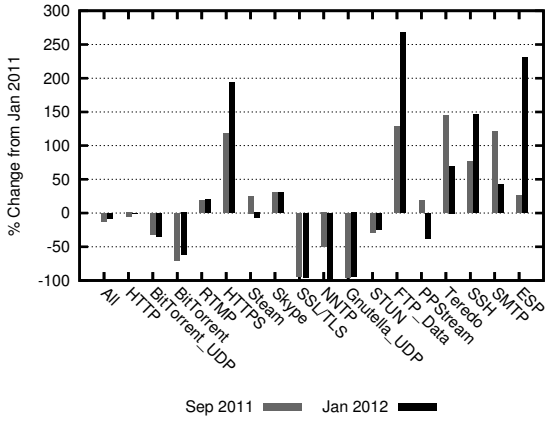

Figure 2: Bytes downloaded by residential DSL subscribers relative to the value observed in January 2011, broken down by application protocol.

4. RESULTS

4.1 Bytes Transferred

Figures 1 and Figure 2 show the quantity of bytes downloaded by residential DSL subscribers relative to the value observed in January 2011, i.e. prior to the CAA coming into effect. Figure 1 shows the analysis on the category level whereas Figure 2 shows the results for a selection of individual application protocols. A category or protocol must have contributed at least one gigabyte per day in order to be included in either graph.

Overall, traffic across all categories decreased 7.5% in January 2012 compared with the volume observed in the previous year. Unencrypted web traffic was mostly static across all three trace sets but HTTPS traffic tripled between January 2011 and January 2012.

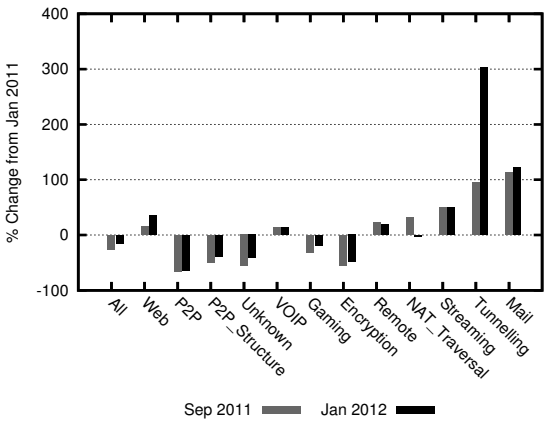

Figure 3: Bytes transmitted by residential DSL subscribers relative to the value observed in January 2011, broken down by application category.

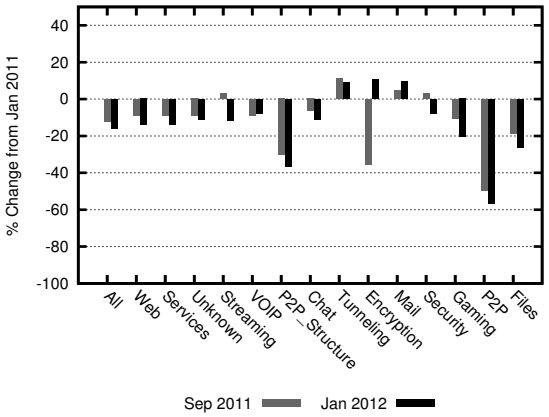

Figure 4: Active residential DSL subscribers using an application from each category, relative to the subscriber count in January 2011.

There were significant decreases in both the P2P and P2P structure categories. Downloaded traffic that was recognisable as P2P fell by 69% between January 2011 and September 2011 and recovered only slightly in January 2012. P2P structure traffic, i.e. P2P network maintenance traffic, was less affected but still decreased by 32% in September 2011. The primary cause for the decrease in both categories appeared to be a decline in BitTorrent usage. Also, Gnutella UDP traffic disappeared almost entirely from the ISP network, accounting for only 5% of the volume that it had in January 2011.

The Newsgroups and Encrypted categories also experienced sharp declines in traffic volumes in September 2011. Binary newsgroups are commonly used for sharing files (including copyrighted material) while many P2P file sharing applications use SSL to encrypt traffic. The decrease in encrypted traffic is likely because encryption does not protect against detection by copyright holders, as they detect infringements by finding New Zealand IP addresses participating in P2P networks that are sharing the copyrighted content. Some major newsgroup providers have been shut down in recent times, e.g. News-Service.com was closed in November 2011 [1], which may have caused the decline in NNTP traffic in the January 2012 dataset.

Unknown traffic also decreased in September 2011, which shows that the file sharing traffic did not move to new undetectable protocols. Rather, the decline in Unknown traffic leads us to believe that the converse may have been true: much of the Unknown traffic in January 2011 may have been encrypted P2P traffic that we were unable to detect using libprotoident.

By contrast, there were large increases in downloaded traffic matching the Files, Remote and Tunneling categories. Figure 2 shows that this was due to the growing use of protocols such as FTP, SSH, ESP (Encapsulating Security Protocol) and Teredo. Another protocol worth mentioning that is not present in Figure 2 is OpenVPN, which was seldom observed in January 2011 but was much more prominent in the later trace sets.

Our belief is that much of the growth in these categories can be attributed to users changing their file sharing approach. Rather than participating in P2P exchanges from home where they can be detected by copyright holders and issued an infringement notice under the CAA, the user downloads files using a seedbox located in a foreign country. The files are then copied directly back to their personal computer using either a secure tunnel, such as a VPN, or downloaded from a secure HTTP or FTP service running on the seedbox. This could also explain the large growth in HTTPS traffic.

While Files, Remote and Tunneling traffic has grown significantly, the total volume of traffic matching those categories was still relatively small compared with P2P traffic, as shown in Table 3. BitTorrent alone was still responsible for more downloaded traffic than any tunneling or remote access protocols. Furthermore, daily BitTorrent traffic decreased by 39 GB between January and September 2011 whereas growth in the daily traffic matching the Files, Remote and Tunneling categories was less than 5 GB for the same time period. Daily HTTPS traffic grew by 13 GB in the same time period, but it is unlikely that the entire increase can be attributed to seedboxes, e.g. online shopping, Internet banking and secure login to social media sites such as Facebook are also likely contributing factors.

Following the enactment of HADOPI in France, many users switched to using illegal streaming to access copyrighted content [10]. We also observed an increase in Streaming traffic in the September 2011 data set but the growth was not enough to suggest an uptake similar to that observed in France. This may be partly due to New Zealand's geographic isolation – the streaming sites hosted are not within New Zealand and the latency to foreign sites would likely result in a poor user experience. Rather, we suspect this increase is the result of increased uptake of legal radio, music and television streaming services which have developed an increased presence in New Zealand recently.

The CAA was also intended to target uploaders of copyrighted material. Figure 3 shows the traffic transmitted by residential DSL users, again broken down by category. Many of the trends observed in downloaded traffic were also present in uploaded traffic, such as the decrease in P2P file sharing and an increase in the Tunneling and Streaming categories. Outgoing Mail traffic had also increased significantly, although it is unlikely that this is related to the CAA.

	Jan 2011		Sep 2011		Jan 2012	
	GBs / day	Percentage	GBs / day	Percentage	GBs / day	Percentage
HTTP	469.3	68.7	441.3	72.3	465.4	70.9
BitTorrent UDP	55.8	8.2	38.0	6.2	36.1	5.5
BitTorrent	54.3	8.0	15.8	2.6	20.5	3.1
RTMP	20.8	3.0	24.6	4.0	24.9	3.8
HTTPS	11.2	1.6	24.3	4.0	32.7	5.0
Steam	10.2	1.5	12.7	2.1	9.4	1.4
Skype	9.1	1.3	11.9	1.9	11.9	1.8
SSL / TLS	7.3	1.0	0.4	0.1	0.4	0.1
NNTP	2.9	0.4	1.4	0.2	< 0.1	< 0.1
Gnutella UDP	2.0	0.3	0.1	< 0.1	0.1	< 0.1
FTP Data	1.1	0.2	2.4	0.4	3.9	0.6
Teredo	0.9	0.1	2.1	0.3	1.5	0.2
SSH	0.4	0.1	0.7	0.1	1.0	0.2
ESP	0.4	0.1	0.5	0.2	1.3	0.2
OpenVPN	< 0.01	< 0.1	1.4	0.2	1.6	0.2

Table 3: Bytes downloaded by DSL subscribers that matched each application protocol. "Percentage" refers to the proportion of traffic in the trace set that matched the protocol.

4.2 Active Users

We also examined the number of subscribers that were actively using each application protocol to assess whether the CAA had caused some subscribers to cease using P2P applications altogether. We defined a subscriber as actively using a protocol if a flow was observed where the subscriber had either transmitted a packet containing application payload or received at least one megabyte of application payload from the external host. The second condition ensured that we did not exclude one-way passive FTP transactions as these do not require the recipient to transmit any data.

Figure 4 shows the relative change in the number of subscribers actively using an application from each of the most prominent categories. Overall, the number of residential DSL subscribers decreased by 16% between January 2011 and January 2012. There is no obvious reason for this decline. The number of subscribers using Web, Services and Gaming traffic, i.e. categories that are largely unaffected by the CAA, fell by a similar amount. By contrast, the number of subscribers using P2P protocols shrank by a much greater amount, halving between January 2011 and January 2012.

Table 4 and Figure 5 show the percentage of subscribers that used certain application protocols and the average volume of traffic downloaded per day by a subscriber when using those protocols, respectively. BitTorrent was not widely used even before the CAA came into effect. Only 8.5% of subscribers actively used BitTorrent in January 2011. Following the enactment of the CAA, this value fell to 5.5% in September 2011 and declined further to 5.2% in January 2012. Also, the amount of traffic downloaded per BitTorrent user also decreased from 126 MB per day per user in January 2011 to 81 MB in January 2012. This matches the behaviour described in [10], where some French Internet users ceased using P2P altogether in response to the HADOPI law while others reduced their downloading activities.

Remarkably, OpenVPN traffic per user went from 600 KB per day in January 2011 to 116 MB per day in January 2012. It is possible that this is due to subscribers using OpenVPN to access seedboxes, although it is difficult to conclusively prove this with the data that we have. OpenVPN was only used by 0.3% of subscribers in January 2012 which suggests

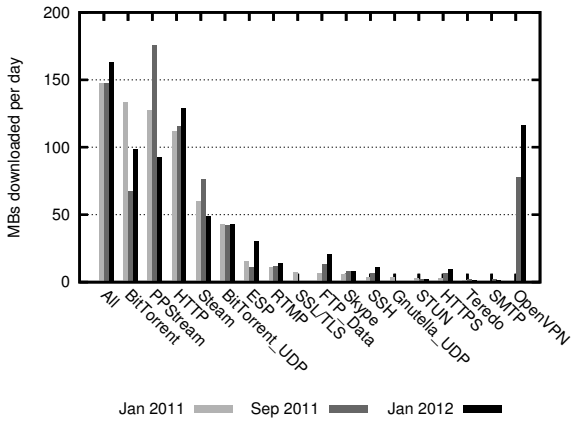

Figure 5: Mean bytes downloaded per day per active user, broken down by application protocol.

that the new usage of VPNs is restricted to a very small group of users. Other tunneling and file transfer protocols that were more popular, such as FTP, ESP and SSH, also exhibited an upward trend in the mean bytes downloaded per user, but the mean values were not as high as those observed for OpenVPN.

Teredo was another major contributor towards the growth in Tunneling usage. However, this is more likely due to the increased presence of IPv6 hosts providing content than P2P being tunneled over Teredo. The amount of Teredo traffic per active Teredo user was much less than what was observed for other Tunneling protocols and did not demonstrate the same upward trend.

5. CONCLUSIONS

In this paper, we presented the results of a study investigating changes in traffic patterns and Internet user behaviour following the Copyright (Infringing File Sharing) Amendment Act (CAA) 2011 which came into effect in New Zealand on 1 September 2011. We used libprotoident, an application protocol classification library, to analyse packet

	Jan 2011		Sep 2011		Jan 2012	
	Subscribers	Percentage	Subscribers	Percentage	Subscribers	Percentage
HTTP	4303	87.3	3919	90.4	3697	89.4
HTTPS	4297	87.2	3905	90.1	3697	89.4
RTMP	1978	40.1	2233	51.5	1802	43.6
Skype	1726	35.0	1580	36.5	1609	38.9
BitTorrent UDP	1348	27.4	926	21.4	858	20.8
SSL / TLS	1067	21.7	689	15.9	1181	28.6
Teredo	939	19.1	1070	24.7	1088	26.3
Gnutella UDP	588	11.9	233	5.4	233	5.6
BitTorrent	418	8.5	240	5.5	213	5.2
Steam	175	3.6	141	4.0	166	4.8
FTP Data	169	3.4	190	4.4	196	4.7
SSH	126	2.6	113	2.6	100	2.4
ESP	27	0.6	47	1.1	44	1.1
OpenVPN	7	0.1	18	0.4	14	0.3
NNTP	5	0.1	2	< 0.1	3	0.1

Table 4: The number of residential DSL subscribers that were using each application protocol in the data sets. "Percentage" refers to the proportion of all active subscribers that used the protocol.

traces captured at a single New Zealand ISP both before and after the law came into effect. In particular, the number of residential DSL subscribers that were using each application protocol as well as the volumes of traffic downloaded and uploaded by those users were examined.

Our main findings are summarised as follows:

- Traffic downloaded using P2P applications decreased to less than half the volume it had been prior to the CAA coming into effect. The decline persisted for several months afterward and many subscribers appeared to have ceased using P2P applications entirely.
- P2P uploads also decreased significantly following the introduction of the CAA. P2P traffic transmitted by DSL subscribers in January 2012 was a quarter of the amount transmitted in January 2011.
- FTP, tunneling and remote access protocols increased in popularity following the introduction of the CAA. The relative growth in these protocols compared with January 2011 was very large, e.g. 300% more tunneling traffic was received by residential DSL subscribers in January 2012 compared to the previous year.
- The number of active subscribers and traffic generated by tunneling, remote access and FTP remained much smaller than the corresponding values for P2P, suggesting that the observed growth in those protocols was not indicative of a widespread change in file sharing behaviour.
- Newsgroup traffic almost completely disappeared after the CAA came into effect, possibly suggesting that NNTP was being used almost exclusively for file sharing.

These results suggest that there is a strong correlation between the CAA coming into effect and the behaviour of New Zealand residential DSL users, at least in the short term. Many subscribers appear to have abandoned P2P file sharing entirely while the remaining P2P users downloaded less content on a per-user basis than they had previously. Other application protocol categories that were related to file sharing, including newsgroups, encrypted traffic and unclassified traffic, also experienced large declines in traffic volume.

Conversely, there was a distinct increase in the use of tunneling, secure file transfer and remote access applications amongst a small group of subscribers. We believe that this may be due to users responding to the CAA by changing their approach to file sharing to limit the likelihood of being detected by copyright holders. Rather than running P2P applications at home, people can use seedboxes located outside of New Zealand to download copyrighted material and transfer the files back to their home computer using HTTPS or a secure tunnel. However, we note that the decrease of P2P traffic observed in our study was much greater than the amount of new traffic that could be associated with tunneling and file transfers.

The results presented in this paper describe the behaviour of subscribers from one New Zealand ISP only. Other ISPs may offer subscription plans and data caps which may appeal more to the people who download copyrighted material. For example, one ISP may be more popular with "heavy" P2P users because they sell a subscription plan with a high off-peak data cap, whereas another ISP may only sell plans that target subscribers with small to medium data or bandwidth requirements. Although we believe that the subscriber base that we have measured is suitably representative, we also acknowledge that this study merely represents a single data point when it comes to evaluating the impact of the CAA overall. A comparative analysis with other New Zealand and international ISPs would ascertain whether the behaviour that we have highlighted is caused by the CAA rather than just strongly correlated.

Another avenue of future work will involve continuing this study over a longer period of time. At the time of writing, only three people have received a third strike under the CAA and the copyright holders elected not to take any of the cases to the Copyright Tribunal. Many copyright holders (in particular, movie and television studios) are not willing to pay the processing fee for issuing notices and the lack of enforcement of the CAA has been widely reported. As a result, it may prove that the decrease in P2P traffic that we have observed will only be temporary.

6. REFERENCES

[1] Curtain falls on News-Service.com (Press Release). http://www.news-service.com/cms/pressrelease20111108en.html (Accessed on 2012/08/16).

[2] Endace Technologies Ltd. http://www.endace.com.

[3] G. Aceto, A. Dainotti, W. de Donato, and A. Pescapè. PortLoad: Taking the Best of Two Worlds in Traffic Classification. In *INFOCOM IEEE Conference on Computer Communications Workshops , 2010*, pages 1 –5, March 2010.

[4] S. Alcock, P. Lorier, and R. Nelson. Libtrace: A Packet Capture and Analysis Library. *SIGCOMM Comput. Commun. Rev.*, 42(2):42–48. April 2012.

[5] S. Alcock and R. Nelson. Libprotoident: Traffic Classification Using Lightweight Packet Inspection. Technical report, University of Waikato. http://www.wand.net.nz/publications/lpireport.

[6] L. Bernaille, R. Teixeira, and K. Salamatian. Early Application Identification. In *Proceedings of the 2006 ACM CoNEXT Conference*, pages 6:1–6:12, 2006.

[7] A. Callado, C. Kamienski, G. Szabo, B. Gero, J. Kelner, S. Fernandes, and D. Sadok. A Survey on Internet Traffic Identification. *Communications Surveys and Tutorials*, 11(3):37 – 52, 2009.

[8] A. Dainotti, A. Pescapè, and K. Claffy. Issues and Future Directions in Traffic Classification. *IEEE Network*, 1(1):35–40, Jan 2012.

[9] B. Danaher, M. D. Smith, R. Telang, and S. Chen. The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France. http://ssrn.com/abstract=1989240, 2012.

[10] S. Dejean, T. Pénard, and R. Suire. Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français. Technical report, University of Rennes, France, 2010. http://recherche.telecom-bretagne.eu/marsouin/IMG/pdf/NoteHadopix.pdf.

[11] Y. Hu, D.-M. Chiu, and J. C. Lui. Profiling and Identification of P2P Traffic. *Computer Networks*, 53(6):849 – 863, 2009.

[12] Internet Initiative Japan Inc. Traffic Shifting away from P2P File Sharing to Web Services. *Internet Infrastructure Review*, 8:25–30. August 2010.

[13] M. Crotti and M. Dusi and F. Gringoli and L. Salgarelli. Traffic Classification through Simple Statistical Fingerprinting. *ACM SIGCOMM Computer Communication Review*, 37(1):5–16, 2007.

[14] M. Pietrzyk and J-L. Costeux and G. Urvoy-Keller and T. En-Najjary. Challenging Statistical Classification for Operational Usage: the ADSL Case. In *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, pages 122–135, 2009.

[15] New Zealand Public Act 11 of 2011. Copyright (Infringing File Sharing) Amendment Act 2011. http://www.legislation.govt.nz/act/public/2011/0011/latest/whole.html.

[16] T. T. T. Nguyen and G. J. Armitage. A Survey of Techniques for Internet Traffic Classification using Machine Learning. *IEEE Communications Surveys and Tutorials*, 10(1-4):56–76, 2008.

[17] M. Perényi, T. D. Dang, A. Gefferth, and S. Molnár. Identification and Analysis of Peer-to-Peer Traffic. *Journal of Communications*, 1(7):36–46, 2006.

[18] T. Pullar-Strecker. P2P downloads fall as 'Skynet' introduced. http://www.stuff.co.nz/technology/digital-living/5578590.

[19] WAND Network Research Group. libprotoident. http://research.wand.net.nz/software/libprotoident.php.