Crab Mentality, Cyberbullying and "Name and Shame" Rankings

Simon Spacey*

19th April 2015(h)

Abstract

This paper examines the hypothesis that in a country where disclosure of higher than average achievement can be considered an appropriate justification for bullying, students are more likely to do badly in exams and collude more in assessed course work to ensure that their grades do not stand out. We examine this hypothesis by measuring how students perform when their position in a class is reported with different levels of perceived privacy. We start by defining what we mean by privacy in rank reporting before discussing a novel rank reporting approach that has higher privacy than traditional approaches. We then provide results for case studies where a traditional and the new higher privacy rank reporting approaches are used with students at a New Zealand university. The results indicate that over 70% of the students are concerned with the privacy of traditional rank reporting approaches and that average student performance may be affected by almost 20% by these concerns.

1 Introduction

CRAB mentality is a behavioural characteristic wherein someone tries to pull down those who are performing better than them. The term comes from watching crabs in a fisherman's bucket. The fisherman can leave the bucket without a lid secure in the knowledge that every time a crab makes progress towards its escape, the others will go out of their way to pull it back into the bucket.

Crab mentality can be seen as a type of envy or hating and is sometimes referred to as tall poppy syndrome from the story of the Roman king Tarquin who was said to have cut the heads off the tallest poppies in his garden as a sign to his son that he should set about secretly assassinating those of achievement around him to ensure his own success (Livius, 2010). But whatever you call the phenomenon, the fact that it is well established and recognised (see for example Comfort, 1995, p. 599) means that:

> standing out through your achievements can cause you to be attacked in some countries.

*S. Spacey is with the Computer Science Department of the University of Waikato in New Zealand (email: sspacey@waikato.ac.nz).

In modern day academia, secretly assassinating your peers is not necessarily performed the same way it was in king Tarquin's day. The growth in importance of social media sites and the simplicity with which anyone can create an account that is not associated with their real identity makes it easier for an attacker to perform assassination through electronic rather than physical means. This form of anonymous electronic assassination is called cyberbullying (Li, 2007; NetSafe, n.d.) and like the assassinations of king Tarquin's time, the harm caused by cyberbullying can include the death of young and old alike (e.g. Bailey, 2014; "Charlotte Dawson's death throws spotlight on cyber bullying", 2014; NOBullying.com, 2013) but does not need to actually kill for its perpetrators to gain advantage in their peer groups as discussed in Vance (2012).

Cyberbullying is such a significant problem in some countries that governments are considering new laws to address it as discussed in "Internet trolls face up to two years in jail under new laws" (2014) for the UK, in US Library of Congress (2013) for the US and in New Zealand, the Harmful Digital Communications Bill (New Zealand Government, 2014) aims to make posting communications with the intent to cause harm punishable by up to 3 months in prison or a $2,000 fine and creates the new offence of "incitement to commit suicide" punishable by up to 3 years in prison.

In this paper we seek to quantify the effect that crab mentality has on the performance of modern students. The hypothesis we examine is that, in a country like New Zealand where crab mentality is an accepted norm (Dediu, 2015; Kirkwood, 2007; Mouly & Sankaranb, 2000, 2002; Tapper, 2014) and even celebrated as a cultural achievement by some (see for example Young, 2009), the addition of cyberbullying creates a perfect storm for underachievement where it is logical for students to fear standing out as tall poppies in rankings and so they will perform worse on average in exams and collude more in assessed course work to increase the chance that their grades are close to others. We test this hypothesis through the introduction of a novel rank reporting approach that allows relative achievements to be published to motivate students and encourage confidence in the assessment process (Bamber, 2014; Lawrence, 2004) while making it more difficult for others to determine the position of a particular student in a ranking without their consent. The novel rank reporting approach is introduced in Section 2 and analysed in Section 3 and we provide survey sentiment and performance impact results from two case studies where students use a traditional and the new rank reporting approach at a New Zealand university in Section 4. The paper concludes in Section 5 with a summary and areas for future work.

2 "Name and Shame" Rankings

The traditional Student Name ranking approach simply provides a list of student names ordered by their position in the class often with a column of actual mark values. The approach has the advantage of being perhaps the most straitforward to understand and use and allows students to quickly identify their own position and show their position in a ranking to others as illustrated in Table 1. However Student Name rankings do not provide any form of privacy at all which is perhaps why New Zealand students call such rankings "Name and Shame" rankings and why many will complain to department heads if a lecturer uses

Table 1: Utility and privacy features of different student ranking approaches. The utility feature columns describe whether an approach allows students to know their own position (Know Pos.) and whether they can use the rankings to show their position to others (Show Pos.). The privacy feature columns describe whether the approach provides: immediate anonymity (Imm.) wherein third parties need additional information to identify students, indirect anonymity (Indr.) wherein a position can be confirmed without disclosing a student's rank on other work, correlation anonymity (Corr.) wherein student group information can not be used to correlate IDs and plausible deniability (PD) wherein a student can deny a rank position proposed for them by others.

	Utility Features		Privacy Features			
Approach	Know Pos.	Show Pos.	Imm.	Indr.	Corr.	PD
Student Name	✓	✓	✗	✗	✗	✗
Student ID	✓	✗	✓	✗	✗	✗
No Rankings	✗	✗	✓	✓	✓	✓
Unique ID	✓	✗	✓	✓	✓	✓
Course Hashes	✓	✓	✓	✓	✓	✓

the approach even where the rankings are only visible to their peers in class.

Because of the lack of privacy in Student Name rankings, most New Zealand universities provide rankings using the Student ID approach today. The Student ID ranking approach can be seen as a simple change to the Student Name approach wherein student names are replaced by their student IDs. Student ID rankings provide the benefit of immediate anonymity which ensures third parties can not identify a student from a ranking without further information. Unfortunately however, the approach has no indirect anonymity in that immediate anonymity is permanently removed from future and past Student ID ranking reports if a student demonstrates their position to others by, for example, showing their student ID card or if a student's position in one ranking is disclosed through a class prize. Further, Student ID rankings are vulnerable to correlation analysis attacks wherein project team members can identify the IDs of other members in shared group results which make Student ID rankings, for all intents and purposes, just another form of "Name and Shame" rankings for modern courses with prizes and group work.

Of course the most secure ranking approach is one that does not exist or is kept entirely private. Unfortunately, while being secure, the No Rankings approach does not allow students to know their own position in a class which could demotivate some students (Lawrence, 2004) and the approach does not allow students to show their position to others which may be required to join some companies (e.g. Goldman Sachs, n.d.; SaSe Business Solutions, n.d.).

A secure alternative to not providing public rankings is to provide rankings with a unique ID for each course work item for each student. This approach has the advantage of allowing the student to know their own position in the class, provides immediate anonymity, correlation anonymity and also provides indirect anonymity and plausible deniability where the unique IDs are randomly

assigned. However the approach has the disadvantage of requiring students to manage multiple IDs and of not providing any way for a student to show their position in a ranking to others without the university providing explicit confirmation of a mapping.

The ranking approach used in this work is called Course Hashes. As Table 1 shows, Course Hashes provide a means to disclose rankings to students in a way that is just as private as Unique ID rankings while allowing students to show their position to a third party like the traditional Student Name ranking approach as discussed next.

3 Course Hash Rankings

Course Hashes were introduced in Spacey (2014) and can be considered a small change to the Student ID ranking approach wherein Student IDs are replaced with new IDs that can be generated using a public function from unique student information. The Course Hash rankings are published openly just like Student ID rankings so that students can use their unique information to generate their Course Hash ID to know and show their position in class to others.

The public function used to generate Course Hash IDs has the general form:

$$\begin{aligned} &\text{publicFunction}(\text{courseID}, \text{workItemID}, \\ &\qquad \text{studentID}, \text{privateKey}) \end{aligned} \tag{1}$$

and combines course, assessed work item and student ID information with a private key to produce an ID of a specified length. The function needs to produce a many-to-one mapping of its inputs to Course Hash IDs using a "one-way function" such as a secure hash (e.g. NIST, 2012) or a cryptographic cypher used in a hashing mode (e.g. NIST, 2001; Spacey, 2001).

The technical merits of one public function implementation choice over another are not important for this work as all that we care about is that it is reasonable to expect that our case study participants would have *perceived* that rankings generated with the above equation will protect their identity *more than* the traditional Student ID approach they were used to. To understand why it is reasonable to expect that our second and third year students will have perceived Course Hashes to be a more secure alternative than traditional ranking approaches (and to supplement the student sentiment results of Section 4.3 which support this assertion in any case), the following sections explain how equation (1) delivers the privacy features of Table 1 and provide some of the theoretical consequences of the Course Hash approach from a student's perspective.

3.1 Immediate Anonymity

The only information in equation (1) that connects a student to an ID is the studentID. Thus as Student ID rankings provide immediate anonymity, and equation (1) has no additional information to identify students, Course Hashes must provide immediate anonymity.

3.2 Indirect Anonymity

The ID generated by equation (1) depends on the work item. Thus a different Course Hash ID will be generated for different work items for the same course, student and private key meaning disclosing a student's ID for one work item (for example through a prize for the top place in the exams) does not directly disclose their ID on other work items. Further, the use of cryptographic hashes makes correlating the known change in input (workItemID1 $\rightarrow$ workItemID2) to a change in the hash's output difficult (see Rogaway & Shrimpton, 2004; Schneier, 1996; Wang, Yin & Yu, 2005) thus providing indirect anonymity.

3.3 Correlation Anonymity

As explained above, equation (1) provides correlation anonymity through the use of cryptographic hash functions. Thus, while students given a group grade may be able to identify the set of possible IDs of other members of their group for a particular course, this information is useless in determining a student's ID in other courses because the use of cryptographic hashes makes correlating the known change in input (courseID1 $\rightarrow$ courseID2) to a change in the hash's output difficult (see Rogaway & Shrimpton, 2004; Schneier, 1996; Wang et al., 2005) thus Course Hashes provide more correlation anonymity than the traditional alternatives.

3.4 Plausible Deniability

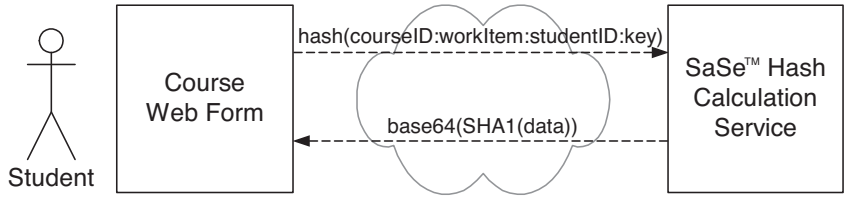
As explained in Spacey (2014), plausible deniability is provided by equation (1) because the private key is constructed to be at least as big (in information terms, see Shannon (2001)) as the range of encoded output Course Hash IDs. This means that any student can be mapped to any Course Hash ID given an appropriate key choice. Or, put another way, finding a key that maps a student to a Course Hash ID does not prove that student has been assigned that Course Hash ID because the key that student has may in fact be different and map them to another Course Hash ID. Thus the students have plausible deniability in that they can deny any supposed ranking by saying the proposer was just lucky in finding a key that mapped them to the ID and, given enough resources or luck, the Course Hash ID (and thus the rank) could have been mapped to anyone in the class.

3.5 Consequences of Course Hashes

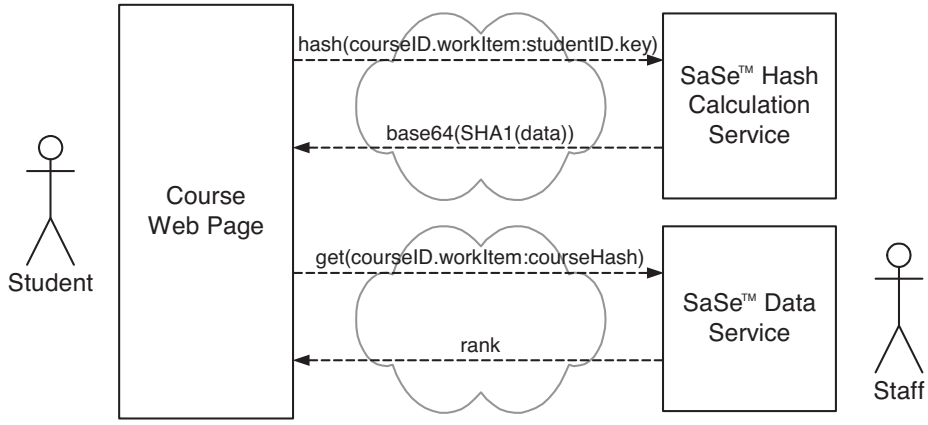
As discussed above, equation (1) provides plausible deniability by including private keys in the public function's inputs to theortically allow any student to be mapped to any Course Hash ID with an appropriate key choice. This presents a challenge for students – namely to find a key that maps them to a higher ID in a Course Hash ranking. However, as Table 2 shows, the usage scenario of the Course Hash function (being to compress private key and student dependent information of fixed length to form a required code rather than, say, to provide a hash to identify substitutions and changes in variable length plain text messages) means that, it would take a considerable time or investment in high-performance computing resources (perhaps using techniques such as Spacey, Luk, Kelly & Kuhn, 2012; Spacey, Luk, Kuhn & Kelly, 2013; Spacey, Wiesemann, Kuhn & Luk, 2012) for a student to find a key that maps them to a higher position in even the 12 Base64 (Josefsson, 2006) character Course Hash IDs used in this work.

Table 2: The repeating random key probability, number of tries and computation time in years before one student is expected to be able to claim the top rank, find a higher rank or for a collision to be seen in the IDs produced using a cryptographically secure Course Hash implementation with 12 character (72 bit) IDs and private keys. The numeric columns assume a class size of 128 students and a Course Hash ID space of 72 bits which are labeled n and N respectively in the probability equations. The Years figure was calculated assuming a machine capable of running a sustained 2^{20} (1 048 576) full hash function calculations and ID comparisons per second with the Course Hash Collision figure requiring 128 hash function generations per try. The figures are only slightly different for non-repeating key tries as discussed in the footnote of Spacey (2014).

Issue	Probability Per Try	Tries	Years
Claiming the Top Rank	$\frac{1}{N}$	$> 2^{65}$	1 147 580
Claiming any Higher Rank	$\frac{n-1}{N}$	$> 2^{58}$	9 036
Collision in Generated IDs	$1 - \prod_{i=1}^{n} 1 - \frac{i-1}{N}$	$> 2^{59}$	2 304 185



(a) First case study's (large class) technical architecture.



(b) Second case study's (smaller class) technical architecture.

Figure 1: Illustration of the Course Hash implementation architectures used in the case studies. The SaSe Secure Hashing Service (see SaSe Business Solutions, 2012) returns a Base64 encoded SHA1 of the passed `data` string from which the first 12 characters (72 bits) are either reported as the Course Hash ID or passed on to the SaSe Data Service (see SaSe Business Solutions, 2012) to get the ranking grade by the Course Web Page JavaScript code.

4 Results

In this section we describe two case studies where Course Hashes were used with students at a New Zealand university and examine the student view of the increased privacy as well as the impact on their performance. In the first case study students used a manual process to generate their Course Hash IDs from their private keys and student information and in the second this process was automated as discussed below. In both case studies a single private key was provided for each student for all the work items of the course. The keys and Course Hash IDs were twelve characters in the case studies to ensure significant challenge to prevent students generating keys to map themselves to higher rankings as discussed in Section 3.4 while remaining practical for students to type by hand if they needed to.

4.1 First Case Study: Large Class

The first case study was with the compulsory second year Computer Systems course at the University of Waikato which had 115 enrolled students of which 104 were male and 11 female and 99 were either Citizens or Permanent Residents of New Zealand and 16 were international students. The course was assessed with technical learning labs and a mid-semester test in the first half of the course followed by project labs and a final exam in the second half. The symmetry between the first (labs and a test) and second (labs and an exam) half of the course allowed us to baseline student performance in the first half of the course with students expecting Student ID rankings and then actually report the fist half results using Course Hashes as a surprise to ensure the students were familiar with the new high privacy reporting approach before they started the second half of the course.

The technical architecture we used in our first case study is shown in Figure 1(a) and involved a three step usage scenario wherein:

1. a student manually gets their private key from Moodle,
2. uses a web form to generate their Course Hash ID and
3. manually looks-up the rank for their Course Hash ID in a published PDF ranking for the work item

The students were divided on the usability of the three step process as explained in Section 4.3 and so the implementation architecture was modified for our second case study as discussed next.

4.2 Second Case Study: Smaller Class

The second case study was with the elective third year Computer Architecture course at the University of Waikato which usually attracts some of the best students from the previous year's Computer Systems course and had 16 enrolled students in the case study year. The students were all male and one was an international student. The course was taught after the first case study completed and, although the students were different, it was expected that news of the Course Hash approach had leaked to the students and so unlike the first case study, we explained from the beginning that Course Hashes would be used for rank reporting and had to use the previous year's results for a baseline to compare the performance of students against.

The course was assessed with a test and lab work items. Unfortunately, while the lectures and test were created by the same lecturer as previous years, the labs had changed considerably and were being taught and assessed by a different lecturer meaning that comparison of the impact on the assessed course work could not be performed. Additionally, there were some changes in the admissions policy for the course that had to be accounted for when calculating the exam impact results.

The technical architecture used in the second case study is shown in Figure 1(b). The architecture automates the usage scenario into a one step process where a student simply clicks on a parameterised url they were e-mailed and the url shows a form which generates the student Course Hash ID from the url parameters and gets the grade and rank for the Course Hash ID from an on-line

database. It should be noted that the second architecture is just as secure as the first because, while ranks are now available in an on-line database in addition to a published PDF file, the database ranks like the PDF ranks are indexed by Course Hash ID rather than by any personal student information such as their student ID or e-mail address and the on-line rank update process illustrated on the right hand side of Figure 1(b) is a secure process that only the lecturer can use.

4.3 Student Sentiment

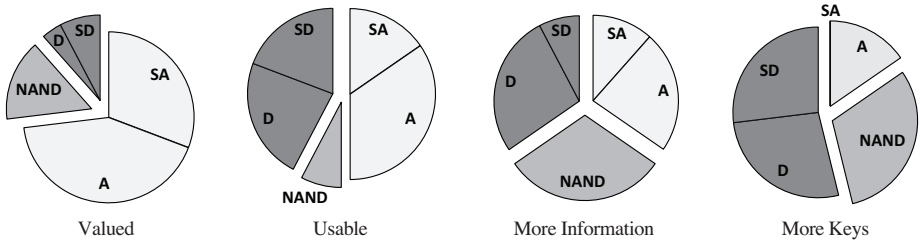
Each case study was followed by a survey to assess the level to which the students:

1. valued this work to increase their ranking privacy,
2. were comfortable using the implementation,
3. would be interested in additional technical details and
4. would prefer per work item private keys instead of the single course level key provided.

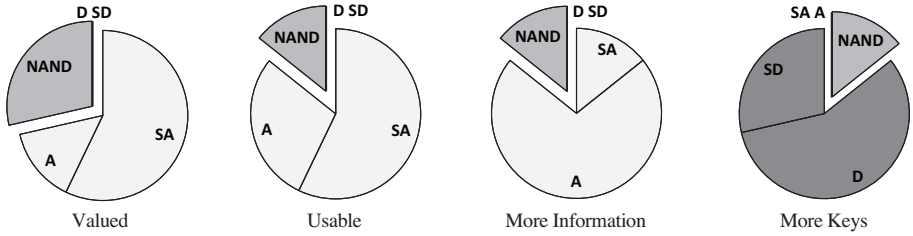
The surveys were created according to the Total Survey Quality (TSQ) design principles (Biemer, 2010) and included sections to collect general feedback on the good and bad points of the students' initial Course Hash experience and any specific suggestions for improving the implementation and the assessment questionnaire itself to identify any TSQ usability issues. To satisfy the timeliness, accessibility, collection completeness and accuracy dimensions of the TSQ requirements and to reduce measurement, item non-response and processing errors we used SurveyMonkey (SurveyMonkey, n.d.) with ranged radio button and free text entry boxes to collect and collate survey responses.

The survey invitation e-mail was constructed according to the Web Survey Invitation Design principles of Kaplowitz, Lupi, Couper and Thorp (2012) and e-mailed to the students after each case study class had ended with two reminders sent over a 1 week period. No prize or inducements were given to complete the survey and 23% of the students in the first (larger class) and 44% in the second (smaller class) case study responded, with the first case study response rates being consistent with the response rates seen for larger student groups in Kaplowitz et al. (2012).

Figure 2 summarises the sentiment survey results. It can be seen that 73% of the respondents in the first case study and 71% in the second stated that they either agreed or strongly agreed that they valued the work to increase their rank reporting privacy, supporting the assertion that students are concerned with the privacy afforded by traditional "Name and Shame" rank reporting approaches and considered Course Hashes an improvement in the privacy afforded by Student ID rank reporting which was the alternative used before Course Hashes by the students. It is perhaps noteworthy that the percentage of respondents who did not actively support the work is consistent with the view that as many as 1 in 5 modern students are cyberbulliers (Li, 2007) and that for these students, an increase in ranking privacy represents a risk to the ego benefits they are deriving from the education system (Vance, 2012).



(a) Sentiment results for the first (large class) case study.



(b) Sentiment results for the second (smaller class) case study.

Figure 2: Pie charts corresponding to the survey results for the questions (from left to right) of whether the students: valued the work to protect their ranking privacy, were comfortable using the implementation, were interested in additional technical details and whether they would prefer individual work item keys to a single key. The labels correspond to the classifications of: Strongly Agree (SA), Agree (A), Neither Agree Nor Disagree (NAND), Disagree (D) and Strongly Disagree (SD).

Looking at the response to the second survey question we see that after the first case study, the students were divided on whether the Course Hash implementation of Figure 1(a) was usable or not. An examination of the text responses indicated that students were dissatisfied with the manual steps required in the process and so we automated the process for the second case study as discussed in Section 4.2 which resulted in a dramatic increase in student usability sentiment as shown in Figure 2(b), which, perhaps because of the increased process encapsulation, was accompanied by an increase in the percentage of students wanting additional technical information about the Course Hash approach.

The last survey question examined if the students would prefer one private key/parameterised Course Hash url for all the assessed work items in a course or a different key/url for each work item. The question explained that with a key for each work item, the students would be able to demonstrate their position to others on a per work item basis rather than disclosing rankings on an entire class level. In both case studies, the students said they would prefer to keep the single key/url per class they were given and it remains for future work to see if a concrete alternate architecture can make a per work item key implementation an attractive alternative for students.

Table 3: Impact of introducing additional privacy in class ranking reports on average student test/exam and assessed course work grades. The $\delta\mu$ and $\delta\sigma$ columns show the arithmetic difference in average student grades and standard deviations after introducing the Course Hash ranking approach in the case studies. The p-value columns show the significance of the results using a paired and unpaired homoscedastic two tail t-test for the first and second case studies respectively.

	Impact on Exams			Impact on Course Work		
Case Study	$\delta\mu$	$\delta\sigma$	p-value	$\delta\mu$	$\delta\sigma$	p-value
1st Larger	**+18%**	**+4%**	0%	-5%	**+4%**	2%
2nd Smaller	**+10%**	**+4%**	1%			

4.4 Impact on Student Performance

Table 3 summarises the impact introducing rank reporting privacy had on the performance of the students in our case studies. In both case studies, the average test/exam marks increased significantly after introducing higher rank reporting privacy and the standard deviation of the assessed course work increased where a comparison was possible. The results are all statistically significant with low p-values and support the hypothesis that: in a country where crab mentality is an accepted norm and where cyberbullying is a recognised problem, students may perform worse on average in exams and collude more in assessed course work to increase the chance that their grades are close to others in a class where there is a perceived risk that their relative achievements could be determined through "Name and Shame" rankings or other means.

Referring to Table 3 we can see from the Impact on Exams columns that the average student test/exam grades increased by 18% for the first case study and 10% for the second after introducing rank reporting privacy with the increase in standard deviation showing the increase was not just a shift, but a widening of the gaps between grades. Looking at the Impact on Course Work columns we see that while the average course work grade dropped after introducing rank reporting privacy, the standard deviation of the course work grades increased which we take to be an indicator that students were prepared to work more independently after ranking privacy was introduced despite, one assumes, having already developed unofficial groups to share individually assessed course work items in the first half of the course when they were expecting Student ID rankings. In the interests of completeness, it should be noted again that the impact on the course work grades could not be calculated for the second case study for the reasons outlined in Section 4.2.

An alternate view of Table 3's results for the first case study are provided in Spacey (2014) where the relative changes in the first and second half grades are compared against the previous year when Student ID rankings were used for both halves of the course. The results are consistent with those of Table 3 and further support the hypothesis. However, taking a cue from Spacey (2014), and noting that the first case study's labs were kept essentially the same as the previous years for this work, it is possible to use the previous year's labs as a

control group to assess the impact of Course Hashes with the same assessments (albeit now with necessarily different students). Doing so reveals consistent results with a decrease in average performance for the second half labs of 6% and an increase in the standard deviation of 7% with an unpaired homoscedastic p-value of 3% (hetroscedastic 4%). For completeness, a comparison between the first half lab results for the two years (when the students were expecting Student ID rankings in both cases) reveals less than 1% average grade difference, 3% standard deviation difference (which when subtracted from the 7% for the second half labs gives us our 4% again) and a p-value of 73% (homo- and hetroscedastic) – all consistent with the hypothesis.

4.5 Discussion

While it may be tempting to extrapolate the results of this work to a wider context, it should be noted that there are a number of difficulties in doing so. First and foremost, it should be clear that this paper like many others is a stepping stone for future research. Our approach is a quantitative approach that maintains the established benefits of public rankings (Bamber, 2014; Lawrence, 2004) while complementing the traditional qualitative approaches used by authors like Tapper (2014) and Li (2007) and without using aspects from both approaches it is difficult to both quantify and claim causality for effects which is why we are careful to only claim *support* for our hypothesis in this paper leaving universal results for future work.

Secondly, it should be noted the year of this study was the year of Charlotte Dawson's death which has been attributed to cyberbullying by New Zealanders ("Charlotte Dawson's death throws spotlight on cyber bullying", 2014). This and other events, while not discussed in class, may well have affected student's perceptions of privacy and the consideration of those effects, including any permanence, remains a topic for future work.

Finally, there is the potential criticism that we used previous assessment results as a baseline for some of our impact figures rather than dividing the students. Unfortunately however, dividing the students would have brought its own issues in:

1. reducing the significance of the survey results given the expected response rates of Kaplowitz et al. (2012),

2. highlighting the possible comparisons to students some of whom (Li, 2007) may have then been motivated to affect the study results and

3. potentially subjecting some students to a relative disadvantage

and while this criticism has already been addressed in Section 4.4 in a way that avoids the above issues, the collection of additional results remains a topic for future work with the knowledge that point 2 may be difficult to address given the release of this paper and the recognised prevalence of crab mentality and cyberbulliers in some cultures as highlighted by the references.

5 Conclusion

In this paper we examined the hypothesis that in a country where crab mentality is an accepted norm and where cyberbullying is a recognised social problem, students may perform worse on average in exams and collude more in assessed course work when there is a chance that their relative achievements can be discovered by others through "Name and Shame" rankings. To test this hypothesis we had to compare how students performed when they were expecting their results to be reported in a traditional "Name and Shame" ranking format and how they performed when they were expecting results reported in a ranking format that they thought other people could not determine their position from. This meant that we needed to detail how people could determine the position of others from traditional rankings which we did in Section 2 and propose a more secure alternate rank reporting approach which we did in Section 3 where we discussed Course Hashes.

In Section 4 we provided results comparing student performance when they expected a traditional rank report and when they expected the new higher privacy report. The results were for two case studies with a total of 131 second and third year students at the University of Waikato in New Zealand. In both case studies over 70% of respondents said they valued our efforts to provide increased rank reporting privacy. This figure is perhaps all the more staggering when you understand that the ranking privacy the students were comparing our increase to was that provided by Student ID rankings and the fact that university's around the world are blindly using Student ID rankings today with the apparent view that the approach provides a satisfactory level of privacy for their students.

In Section 4.4 the impact on student performance of increasing rank reporting privacy was provided. The results were all statistically significant and showed up to 18% increase in average student test/exam performance with a, surprisingly consistent, 4% increase in course work standard deviation indicating students trying harder and working more independently in response to increased ranking privacy.

While the sentiment surveys and performance impact results of this paper support the hypothesis and are consistent with other work (Dediu, 2015; Feather, 1989; Kaplowitz et al., 2012; Kirkwood, 2007; Li, 2007; Tapper, 2014), the difficulty in obtaining universal results has to be recognised as discussed in Section 4.5. Additionally, it should be understood that the case studies were both performed with technically focused students and that crab mentality and the public cyberbullying of students, teachers and others are such established cultural norms in New Zealand (see for example Bailey, 2014; "Charlotte Dawson's death throws spotlight on cyber bullying", 2014; New Zealand Government, 2014; Tapper, 2014; Vance, 2012; Young, 2009) that some educational institutions and unions may even act to prevent investigation into cyberbullying cases when they perceive a cultural justification through crab mentality (Bing, 2014; Dougan, 2015 and see also Mouly & Sankaranb, 2002). Thus it remains for future work to assess if the sentiment and performance impact results presented in this work cross student discipline, geographic and other boundaries in addition to examining the relative merits of alternate technical implementations.

Acknowledgment

The feedback on earlier working versions of this paper provided by anonymous reviewers is greatly appreciated.

References

Bailey, A. (2014, 24th February). Cyber-bullying blamed for death. *The New Zealand Herald*.

Bamber, M. (2014). The impact on stakeholder confidence of increased transparency in the examination assessment process. *Assessment & Evaluation in Higher Education*, *40*(4), 471–487.

Biemer, P. (2010). Total Survey Error: Design, implementation, and evaluation. *Public Opinion Quarterly*, *74*(5), 817–848.

Bing, D. (2014, 19th August). Waikato branch newsletter #9. *New Zealand's Tertiary Education Union (TEU)*.

Charlotte Dawson's death throws spotlight on cyber bullying. (2014, 23rd February). *ONE News*.

Comfort, N. (1995). *Brewer's politics: a phrase and fable dictionary.* Cassell.

Dediu, A. (2015). *Tall Poppy Syndrome and its effect on work performance* (Masters thesis). University of Canterbury, New Zealand.

Dougan, P. (2015, 2nd June). Uni lecturer to challenge employer over cyberbullying. *The New Zealand Herald*.

Feather, N. (1989). Attitudes towards the high achiever: The fall of the tall poppy. *Australian Journal of Psychology*, *41*(3), 239–267.

Goldman Sachs. (n.d.). *Summer analyst internship: Who can apply.* Retrieved 30 January 2015, from `http://goo.gl/SHVSX8`

Internet trolls face up to two years in jail under new laws. (2014, 19th October). *BBC News*.

Josefsson, S. (Ed.). (2006). *The Base16, Base32, and Base64 Data Encodings* (Standard No. RFC 4648). Internet Engineering Task Force (IETF).

Kaplowitz, M., Lupi, F., Couper, M. & Thorp, L. (2012). The effect of invitation design on web survey response rates. *Social Science Computer Review*, *30*(3), 339–349.

Kirkwood, J. (2007). Tall Poppy Syndrome: implications for entrepreneurship in New Zealand. *Journal of Management & Organization*, *13*, 366–382.

Lawrence, R. (2004). Teaching data structures using competitive games. *IEEE Transactions on Education*, *47*(4), 459–466.

Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology*, *23*(4), 435–454.

Livius, T. (2010). The history of rome. In *1.54.* Digireads.com Publishing.

Mouly, V. & Sankaranb, J. (2000). The tall poppy syndrome in New Zealand: An exploratory investigation. *Transcending boundaries: Integrating people, processes and systems*, 285–289.

Mouly, V. & Sankaranb, J. (2002). The enactment of envy within organizations: Insights from a New Zealand academic department. *The Journal of Applied Behavioural Science*, 36–56.

NetSafe. (n.d.). *Cyberbullying information and advice for teachers and principals.* New Zealand Ministry of Education Sponsored White Paper.

New Zealand Government. (2014). *Harmful Digital Communications Bill.*

NIST (National Institute of Standards and Technology). (2001). *Advanced Encryption Standard (AES)* (Standard No. FIPS PUB 197). Gaithersburg, MD.

NIST (National Institute of Standards and Technology). (2012). *Secure Hash Standard (SHS)* (Standard No. FIPS PUB 180-4). Gaithersburg, MD.

NOBullying.com. (2013, 23rd April). *Six unforgettable cyberbullying cases.*

Rogaway, P. & Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance and collision resistance. In *Proc. fast software encryption (FSE)* (Vol. 3017, pp. 371–388).

SaSe Business Solutions. (n.d.). *General questions.* Retrieved 8 August 2014, from `http://www.sase.biz/faq.html`

SaSe Business Solutions. (2012). *SaSe Server Pages (SSP)* [Product Information Sheet].

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley.

Shannon, C. (2001). A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, *5*(1), 3–55.

Spacey, S. (2001). *The Spacey Cypher* (UK Patent 2379587B).

Spacey, S. (2014). Selectively anonymous rankings: Design, analysis and impact on computer science students. In *Proc. of the IEEE international conference on teaching, assessment, and learning for engineering (TALE).*

Spacey, S., Luk, W., Kelly, P. & Kuhn, D. (2012). Improving communication latency with the Write-Only Architecture. *Journal of Parallel and Distributed Computing*, *72*(12), 1617–1627.

Spacey, S., Luk, W., Kuhn, D. & Kelly, P. (2013). Parallel partitioning for distributed systems using sequential assignment. *Journal of Parallel and Distributed Computing*, *73*(2), 207-219.

Spacey, S., Wiesemann, W., Kuhn, D. & Luk, W. (2012). Robust software partitioning with multiple instantiation. *INFORMS Journal on Computing*, *24*(3), 500–515.

SurveyMonkey. (n.d.). *Home page.* Retrieved 30 January 2015, from `http://www.surveymonkey.com`

Tapper, L. (2014). *'Being in the World of School'. A Phenomenological Exploration of Experiences for Gifted and Talented Adolescents* (PhD thesis). University of Canterbury, New Zealand.

US Library of Congress. (2013). *Tyler Clementi higher education anti-harassment act.*

Vance, A. (2012, 15th August). Proposed laws target cyber-bullying. *Stuff.co.nz*.

Wang, X., Yin, Y. & Yu, H. (2005). Finding collisions in the full SHA-1. In *Proc. advances in cryptology (Crypto)* (pp. 17–36).

Young, B. (2009, 11th November). Tall Poppy Syndrome – our best invention? *The New Zealand Herald*.