Submission

Criminal Procedure Reform and Modernisation Bill

Tech Liberty
http://techliberty.org.nz
14th February 2011
PO Box 5641, Lambton Quay, Wellington

About this submission

The Bill encompasses a wide ranging reform of criminal procedure in New Zealand. A relatively small, but important part falls within the scope of interest of this submitter (Tech Liberty).

This submission focuses on Subpart 3 of Part 5 of the Bill, dealing with "Public access and restrictions on reporting", an issue that has attained some prominence in the context of fast developing communication technologies and the consequent new means of social interaction. These developments trigger a debate about the principles of our (criminal) justice system.

In this submission we will address the human issues of civil liberty separate from the technical perspective. We will use the technical perspective to demonstrate the impracticalities, or even futility, of failing to take a principled approach in respect of the former.

About the submitter

Tech Liberty's mission is to defend civil liberties in the digital age. We are a group dedicated to protecting people's rights in the areas of the Internet and technology. We make submissions on public policy, help to educate people about their rights, and defend those whose rights are being infringed.

Oral Submission

Tech Liberty would like to be heard on this submission.

Contact Details

Enquiries can be directed to Tech Liberty's spokesperson, Thomas Beagle, on 021-80-50-40 or at thomas@techliberty.org.nz. Questions about this submission can also be directed at Dr Berry Zondag, on 07-868-4800 or at berry@zondag.co.nz.

General comments, the principle of open justice, restrictions on reporting

We particularly emphasise that a justice system and the laws that it upholds are only as robust as the opportunities to observe the law and its institutions in action, and the consequent opportunities to have an open and well informed debate.

While acknowledging the potential drawbacks of excessive or prurient interest in some criminal matters, it must be realised that this fundamental debate has been concluded a long time ago, and that our system is what it is as a result. By encroaching ever further on very principal tenets of our system a real risk is created that the end result simply can no longer comply with its most important foundations. In other words, by resolving, in piecemeal fashion, what are considered disadvantages of open justice, we may well end up with a system that does no longer deserve of the very term "justice".

Secondly, and apart from protecting a small class of victims (e.g. children), the openness of justice also has an important function in deterring offenders, those making unfounded or debatable allegations, and those prosecuting them. Again, the advantages and disadvantages in this respect are simply part of the system, which will lose its overall integrity by well-meant, but one-sided, adjustments.

Thirdly, and as expressed in the Law Committee's report, there is a clear public perception that courts too easily depart from the principle of open justice. The associated reduction of confidence in the court system is further aggravated by the relatively simple and often widespread dissemination of information that is sought to be restricted by the courts. The result is not only that the courts are seen as overly restrictive and as encroaching on the basic principle of openness, but that they are also incapable to actually contain what they seek to protect and are in fact virtually powerless in its enforcement. The emperor of suppression of information has few clothes.

Pursuing increasingly draconian punishment for those distributing information, or even for those who (often unwittingly) provide the technical means for such distribution, is unlikely to improve this negative image. The courts would only be seen to be excessively severe for what is often relatively minor transgressions, while technical developments will make it increasingly difficult to apprehend and convict those offending. The courts would therefore only manage to further damage their already tarnished image, without obtaining any practical gains.

The obvious solution to this problem is a stricter adherence to the principle of open justice: where no information is withheld there is no need to have rules about exceptions or their enforcement. While we acknowledge that situations can be construed where the end result of absolutely open justice could be undesirable, by allowing exceptions and the introduction of open-ended discretion similarly unwanted outcomes could result that would lack any principled defence (as opposed to legislated and specified exceptions to openness, such as those of cl205). In our view the choice ought to be for the approach that best preserves the integrity of the system and the rule of law, preferably by abolition of any and all discretion in granting suppression orders.

While a principled solution is therefore possible we realise that this may not be tenable in the current circumstances. Hence a need remains for some powers to grant suppression orders or to restrict access to information. We note that the proposed legislation seeks to create a high threshold in that respect. We would advocate that suppression orders cannot be issued for an

indeterminate term, but that a maximum term is introduced after which orders will lapse unless the court decides otherwise on application by those affected by the orders.

We further oppose the suggestion that a separate class is constructed for members of the traditional media, who will have more ability and standing to query decisions to restrict openness. We will elaborate on this below.

We therefore make the following recommendations:

1. *Reduce all possibilities to restrict access to proceedings and suppression of information to specific circumstances, expressly defined in this legislation, and remove discretionary powers in that respect.*
2. *Provide that all suppression orders have a limited term, and establish that term in this legislation; provide for a process for application for extensions.*

Specific comments, civil liberties and suppressing information

Interpretation for Subpart 3, cl 198 "identifying information"

Although the effect of this definition may be curtailed by the interpretation of cl199, we submit that this definition is unworkable in practice for the following (non-exhaustive) reasons:

First, the terminology "identifying information" is undeterminably wide, in conjunction with "other publicly available information". Information that would qualify as identifying information may be utterly trivial and may have been posted without any intent to identify any person or thing. By way of an example, a simple listing in the white pages could become identifying information if combined with (limited) address information publicly available elsewhere. Information available on a celebrity website about birth dates, descriptions of events, or family circumstances, could become identifying information when combined with the type of information that is customarily included in newspaper reporting.

Secondly, information can take many formats, and examples already exist where identifying information took the shape of hexadecimal code or pictograms. Those examples were obviously crude and simple to decipher, but more advanced approaches can easily thwart the suppression objectives of this legislation.

Thirdly, non-offending information can become identifying information as a result of unrelated later publication of additional information. In such cases culpability will be extremely difficult to determine and establish, and there may well be a complicated chain of small bits of information published by different individuals through different media and channels that ultimately provides a sufficient identifying picture.[1] The ordinary approach to criminal liability in such a complex event would result in a range of individuals with potential liability, each possibly unaware of their role in providing a piece of the eventual "puzzle", the solution of which breaches suppression orders. The advance of search engines and other means of collating (often apparently unrelated) information by using extremely advanced algorithms, is unstoppable, and will make it increasingly simple to find a needle of identifying information in the haystack of global databases and social media. By way of examples, in virtually all recent high profile suppression cases, the identity of the "celebrities" involved could be easily traced, in a matter of minutes.

Interpretation for Subpart 3, cl 199 "the context of prohibited publication"

The bill explicitly seeks to avoid defining "publication", under the assumption that this term can develop at common law. The significant problem with that approach is that it will create substantial legal uncertainty in the context of fast developing communication technology. It is observed that new means of communicating (and thus "publishing") are invented and become mainstream well within the cycle of processing an offence and any subsequent appeals (e.g. Facebook, Twitter). The result will therefore be a perpetual uncertainty of the law, which is in strong contrast with the "rule of law", one of the grounding principles of our legal system.

[1] It must be noted in this context that information on the internet does not "die" as it does in traditional media, even if it removed on purpose. Due to caching, most information placed online, will remain there indefinitely, especially since the costs of increasing data storage is less than the costs of selecting and removing information.

It has been suggested in the media that private conversation falls outside the scope of suppression orders due to the limited audience of such communication. However, even 'private' communication will increasingly lead to the creation of a (semi) permanent record, with a distribution that may well go beyond what the initial communicators were intending - or were perhaps even aware of. An offence may be committed without the offender being aware they have "published" information within the suggested open-ended definition. The offence of publishing thus effectively becomes one of strict liability, which is clearly not in accordance with the gravity of the proposed punishment and the general presumptions of criminal justice.

Cl 199 seeks to limit the effect of cl198 by providing that publication of identifying information can only be in breach when that publication occurs in the context of providing an account or record of the relevant proceeding. The terminology "in the context" is ambiguous and leaves opportunities to breach suppression orders while staying within the apparent meaning of the law. By way of an example, a 'tweet' with the following content would be arguably within the law in the summer of 2010-2011, while carrying a clear message breaching an existing suppression order: "I enjoyed the coverage of the soccer world cup last year, especially the presenter, who showed some real agility kicking the ball at the end of every show". It would be virtually impossible to demonstrate that this communication was made in the context of any report or account of proceedings, unless a potentially enormous string of additional information would be allowed in evidence.

The definitions of clauses 198 and 199 thus invite a level of gamesmanship that will only assist to lower the respect for the courts and the law, and that is bound to lead to what will be perceived as highly selective prosecution. Examples of gamesmanship can be found in the "Trademe" discussion panels and the sites that mirror these, and in the recent "Whaleoil" case. The latter case also provides an example for the selective prosecution problem, as some of the identifying information in that case only operated in an identifying fashion in combination with other information, the publication of which did not result in prosecution.

Given these contextual problems and those relating to identifying information, we suggest that the offence that is defined in cl215 should not be a strict liability offence of publishing certain (undefined) information in a certain (undefined) context, but an offence of intentionally seeking to breach suppression orders. by revealing information, after a suppression order has been issued, that, in addition to what has been released in the suppression order itself, or to what was in the public domain at the time of the suppression order, could reasonably lead to the identification of those protected by the order or the information that is suppressed by the order. We suggest that this approach would provide a better determinable objective element (actus reus) as well as introducing a subjective element (mens rea). We note that this offence could conceivably be located in the Summary Offences Act or the Crimes Act. We therefore recommend:

3. *Change the offence created in cl215 to one aimed at the purpose of the offending (breach of an order), rather than at its indeterminable publication aspect.*

Exception for members of the media, cl202; standing for media, cl 214

Clauses 202 and 214 seek to create an exception for "members of the media", citing a reference to an unspecified code of ethics and complaints procedures of the Broadcasting Standards Authority or the Press Council.

One of the significant social developments that have resulted from evolutions in communication technology is the ascent of social media and the associated emergence of citizen journalism that covers a broad spectrum, from individuals who publish their thoughts and opinions,[2] to commercial organizations that utilise new means of communication to reach significant audiences,[3] to sites that provide "comments" sections associated with other activities.[4] Many of these "new media" have grown to easily surpass the scope, depth and reach of organisations that would satisfy the definitions of clauses 202 and 214. Additionally, "traditional media" and their journalists have extended their operations into the realm provided by technical developments, thus creating a hybrid environment that encompasses both traditional and new means of disseminating information.

It is apparent that the approach of clauses 202 and 214 seeks to restrict access to information to the "traditional media", thus excluding those privileges from those that should be able to exercise their right to obtain and distribute information under a truly open system of justice. Neither the current bill, nor its explanatory notes, provide any reason or argument to support this policy. We submit this is in direct contrast to the principle of open justice and rights guaranteed under the New Zealand Bill of Rights Act 1990.

We submit that the current draft is an attempt at returning to a status quo that is in contradiction to social and technical developments, encompassing a view of legislative ability that is simply out of touch with reality. Its only effect will be a further diluting of the confidence in the justice system, especially in the context of the rather draconian punishment of offenders against this backward looking legislation.[5]

4. *Remove the special standing for traditional news media.*

[2] And typically allow readers to comment and engage in discussions.

[3] By way of an example, the "Huffington Post", an entirely online newspaper, reaches over 25 million unique monthly visitors, and was recently sold for more than $300 million.

[4] For instance auction sites, such as Trademe.

[5] We do not address another possible argument against the current approach, namely that it creates unequal commercial opportunities to existing media to the detriment of more innovative approaches to communication.

Liability of internet service providers

It appears that the proposed legislation recognises the difficulty of its attempt to directly address those who seek to obtain and distribute information about the operation of the justice system or the cases it deals with, by extending criminal liability to organisations that provide communication services. To that end a definition is introduced for "Internet service provider", which is incomprehensibly broad, especially when seen in the context of ongoing technical development.

In the current state of development, it is virtually impossible for any provider of hosting or communication services to determine and evaluate the content of information stored or transmitted through its infrastructure. The proposed legislation does not at all address the practical means by which a service provider would be able to assess whether any information it stores or transmits might be in breach of any stipulation of the legislation, or how it might ascertain whether any allegation to that effect is valid. In practice, service providers would be forced to remove information or block access to information solely on the basis of an allegation. We submit that this is in direct contrast to proper procedure and rights guaranteed under the New Zealand Bill of Rights Act 1990.

In addition, service providers will be compelled to undertake significant activity for which they will not be compensated, and which may well be in breach of the contractual terms under which they operate. Service providers who acted on an allegation or their own initiative and blocked access to, say a commercial website, would open themselves to contractual liability. The obligation to inform users that information has been removed or that access to material has been blocked, places a further burden on service providers, the extent of which is difficult to assess without further details of how the legislature actually suggests this would operate in practice.

Furthermore, a system where a mere allegation would lead to blocking information is open to abuse by those who might seek to suppress information even without a suppression order in place.

Technical issues and the questions that these raise

The definition of an ISP

As mentioned above, this definition is exceptionally broad, and in strong contrast with the common understanding of the term ISP. The proposed definition would effectively match every individual or organisation that allows transmission of information through its infrastructure, which, in practical terms, is virtually every owner of IT infrastructure, from an individual with a wireless router that is used by more than one person, to global companies with data centres around the world. Technical developments will rapidly increase the potential sphere caught under this definition, with the upcoming rapid development of portable devices (such as state of the art cell phones) that can support data communications for a number of "tethered" computers or even smaller devices, such as e-book readers or tablets. Any attempt to monitor, let alone regulate what goes on in this exponentially increasing global network is by definition futile.

The way websites are hosted on the internet

We wish to further comment on some of the technical problems inherent in the approach taken by the bill. In particular, there are some real problems with the practical implementation of the requirements in clause 216 concerning ISP liability. While the bill requires an ISP to delete or block

access to suppressed information, often the ISP will not actually have the ability to do this without taking down an entire website or even a number of websites. This is obviously disproportionate and we assume that this is not the intended aim of the bill.

To explain why this is we will first have to consider how ISPs host websites. There are four main different ways that a website can be hosted on the Internet, and each of those present different ways in which an ISP is capable of removing information. It must be noted that normally only the people who actually run (i.e. "own") the website can control the content that is published on the website. For example, if someone hosts a blog website on an ISP's server, the ISP is only providing the infrastructure. The ISP will not have the necessary user account and permissions to login to the blog to delete a comment or article that reveals suppressed information.

The following table will be instructive:

	How the website is hosted	**How information can be removed from it**
1	Website run by the ISP on one of their own computers.	The ISP will be able to delete the suppressed information.
2	Website run by someone on a computer owned by the ISP.	The ISP will not be able to delete the information, but will be able to disable the entire website.
3	Website run by someone on a computer owned by another customer of the ISP (most small websites share large servers run by someone else).	The ISP will not be able to delete the information or disable the website, but will be able to disable the computer (and thereby disable all of the websites running on it).
4	Website run by someone on their own servers at a private location (typical of companies with large or complex websites).	The ISP will not be able to delete the information, disable the website or the computer, but will be able to disconnect the customer (thereby taking away their internet connection and disabling their business).

In addition, if an ISP disables a website or multiple websites in an attempt to remove one piece of information, they will be opening themselves up to being sued for breach of contract by the innocent customers who have had their websites affected. This means the ISP will be caught in a very uncomfortable catch-22 – they can't remove the suppressed information directly but if they do remove it by disabling a server they will lose customers and risk being sued. There is no easy way to rectify this situation and retain ISP liability, as this architecture is built into how the internet industry works all across the world.

National v international service providers

Even if it were possible to control what goes on within New Zealand, information does not abide by geographical boundaries. There is nothing to stop a "Wikileaks" approach to disclosing suppressed information. We suggest that the only reason that a "disclose_court_suppression.com" website is not yet operating on a foreign server is that nobody has yet taken the ten-minute trouble to set something like that up, in full anonymity and for very little cost. Foreign ISP's, particularly in countries that do not have suppression laws, or giant web service providers will not adhere to New

Zealand court orders, let alone to simple allegations from New Zealand. It is even more unlikely that foreign service providers will engage in the notification obligations of the proposed law.

The speed of dissemination

A feature of web-based information and social networks is the increasing speed by which information finds its way to very large numbers of users. Good examples are provided by recent natural disasters or social events, where informal networks are consistently faster than traditional media in providing coverage as events happen. That coverage now includes pictures and even audio and video signals.

The number of handheld devices that can record such information and directly transfer it to international networks is ever increasing. It is not a theoretical scenario to assume that many events will increasingly be recorded and transmitted before suppression orders are even contemplated. Pictures of the "celebrity" being arrested or arriving at the court can have been viewed thousands of times before a judge or registrar is aware of the possibility that suppression orders may be sought.

The liability of ISP's, conclusion

We conclude that the idea of creating liability for ISPs is unworkable in practice, and futile in its effect, and therefore recommend:

5. *Remove ISP liability and obligations on ISPs by deleting cl 216*

Conclusions

From a civil liberties perspective, the bill as currently formulated represents an intrusion into the free flow of information in society that is well beyond what is reasonable in a modern democracy.

The bill also starts from an unrealistic view of what legislation can achieve, and we suggest that the state of technology and ongoing developments render the suppression clauses of the bill virtually meaningless. We suggest that the offence that is sought to be created is unworkable in practice, and should be replaced by an offence with well defined objective and subjective criteria.

We particularly object to making internet service providers (especially under the very wide definition that is proposed) agents of the state in suppressing information that should as a matter of principle be open and accessible to all.

We summarise our recommendations as follows:

1. *Reduce all possibilities to restrict access to proceedings and suppression of information to specific circumstances, expressly defined in this legislation, remove discretionary powers in that respect.*
2. *Provide that all suppression orders have a limited term, and establish that term in this legislation; provide for a process for application for extensions.*
3. *Change the offence created in cl215 to one aimed at the purpose of the offending (breach of an order), rather than at its indeterminable publication aspect.*
4. *Remove the special standing for traditional news media.*
5. *Remove ISP liability and obligations on ISPs by deleting cl 216*