

## **FAQs - Harmful Digital Communications Bill**

### **What are harmful digital communications?**

Harmful digital communications, cyber bullying and digital harassment can take a variety of forms.

Examples include sending or publishing threatening or offensive material and messages, spreading damaging or degrading rumours, publishing invasive and distressing photographs, and harassing and intimidating people.

Common digital communications methods include emails, texts, phone messages, blog sites, forums and social media sites like Facebook or Twitter.

The internet and digital technology provide a forum for a unique form of harassment that is easy to create and distribute and difficult to remove.

### **Is harmful digital communications and cyber bullying a big problem in New Zealand?**

In its report, the Law Commission found that 1 in 10 New Zealanders have experienced harmful communications on the internet. That number doubles for those aged between 19 and 29. Other research shows that 1 in 5 New Zealand high school students experienced some form of cyber bullying or harassment.

### **Why is the Government proposing to protect victims of cyber bullying and hold perpetrators to account?**

Bullying is not a new problem, but its reach and impact has increased considerably in the digital age.

The devastating impact of cyber bullying cannot be underestimated, particularly on young people. It is contributing to increased truancy, failure at school and emotional problems such as depression, selfharm and suicide.

Last year, Justice Minister Judith Collins asked the Law Commission to fast-track its work on harmful digital communications as part of its report on new media: *The News Media meets 'New Media': Rights, responsibilities and regulation in the digital age*.

Minister Collins received the Law Commission's recommendations, *Harmful Digital Communications* briefing paper in August 2012, and in April the Government announced a suite of proposals to tackle cyber-bullying.

Minister Collins has introduced the Harmful Digital Communications Bill into Parliament to give effect to those proposals.

## **What does the Bill do?**

The Bill:

- Creates a new civil enforcement regime that includes setting up or appointing an approved agency to be the first port of call for complaints.
- Allows people to take serious complaints to the District Court, which will be able to issue sanctions such as take-down orders and cease-and-desist notices.
- Makes it an offence to post a harmful digital communication with the intent to cause harm, punishable by up to 3 months imprisonment or a \$2,000 fine.
- Creates a new offence of incitement to commit suicide, even in situations when a person does not attempt to take their own life, punishable by up to 3 years imprisonment.
- Provides a “safe harbour” to clarify whether a person hosting the content of others online is liable for content created by others.
- Amends the Harassment, Privacy and Human Rights Acts to ensure they are up-to-date for digital communications.

## **What are the changes to the criminal law?**

The changes will ensure harmful communications are covered by relevant criminal and civil law, regardless of whether they are conveyed or distributed digitally or via “offline” mediums. The changes will also future-proof the laws against technological advances, to make sure they do not become outdated.

The proposed changes largely mirror the Law Commission’s recommendations and include:

- Creating a new offence of posting a harmful digital communication the intent of causing harm.

It would apply to communications that are grossly offensive or indecent, obscene, menacing or knowingly false. The offence will also cover serious instances of intimate recordings being published online without a person’s consent. It will carry a maximum penalty of up to 3 months’ imprisonment or a \$2,000 fine.

The United States, United Kingdom and Australia already have similar offences that criminalise communications that cause serious distress or mental harm.

- Making it an offence to incite a person to commit suicide, in situations when they do not attempt to take their own life.

The offence will be punishable by up to 3 years’ imprisonment. Currently, it is only an offence to aid, abet or incite suicide if a person attempts or commits suicide.

The new, separate offence recognises the distress such provocation can cause and sends a message that the potential consequences of this kind of harassment are too serious to ignore.

The Law Commission had also recommended the creation of a new sexual grooming offence to protect children and young people.

The current sexual grooming provisions in the Crimes Act require that the defendant must have met the young person they have targeted, travelled to meet them, or arranged for or persuaded the young person to travel to meet them.

The Law Commission recommend amending the law to focus on the process of grooming itself, such as exposing a person under the age of 16 to indecent material with the intention of making it easier to lure the young person into unlawful sexual activity.

That proposal overlaps with the new offence of indecent communication with a person under 16 that will be inserted into the Crimes Act 1961 by the Objectionable Publications and Indecency Legislation Bill. The Law Commission is comfortable that that new offence covers the targeted behaviour.

### **Why establish a new civil enforcement regime?**

This was one of the Law Commission's key recommendations. The Government agreed that in the realm of digital communications, better legal options for addressing complaints and taking action were needed. For example:

- Court cases can take a long time. Often the offending material has already done damage and the person who was harmed just wants it removed as soon as possible.
- People may be unwilling to lay a complaint with the police and police may have limited ability to investigate and prosecute such cases.
- Victims may not have the money or inclination to take a civil law claim, such as suing someone for defamation.

### **What role would the proposed new “approved agency” play in the civil enforcement regime?**

Complaints about harmful digital communications will initially be made to the approved agency. Its role includes:

- Advising people on steps they can take to resolve a problem and whether they may have grounds to make a complaint.
- Investigating substantial complaints and attempting to reach settlements between the complainant and the person responsible.

- Liaising with website hosts, ISPs and other internet intermediaries and requesting them to takedown or moderate posts that are clearly offensive.
- Referring serious, unresolved matters to the District Court.

It is anticipated that the approved agency will resolve the majority of cases involving young people.

### **Will the agency investigate all complaints?**

The agency will be able to decline to investigate some complaints, such as:

- when the content of the communication is seen as unlikely to cause harm;
- the complaint is trivial, frivolous or vexatious; or
- investigating the complaint would be unlikely to uphold or enhance the communication principles.

### **Who will be the approved agency and how will they be funded?**

As the Bill progresses through Parliament, the Ministry of Justice will carry out further work to determine the appropriate agency, the exact amount of funding required, and where the funding will come from.

The Bill allows the government to designate any organisation or government body as the approved agency, but the agency has not yet been determined or selected.

### **What is a “safe harbour”?**

The government has included a “safe harbour” provision in the Bill for third parties who host online content. It clarifies when a host can be liable for harmful content that is created and put on their website by another person. An “online content host” could be a range of people – from a news website like Stuff that allows people to comment on stories, to a website like Trade Me that hosts forums, to a blogger who allows people to comment on their blog.

Some recent court cases in New Zealand and overseas that say a content host could be taken to court for the comments put on their website by another person, even if that content host doesn’t actually know about those comments.

The safe harbour will mean that a host is not able to be taken to court for the comments put on their website unless they:

- have been notified by the complainant that the comments are a breach of the law; and
- don’t remove it within a reasonable time.

The approved agency will be able to notify the content host on behalf of a victim and provide them advice and assistance.

A host also has to make sure that a person accessing their content can easily report a complaint. This may include having a button on a webpage to make complaints, or having clear links to a form to complain.

### **What role will the District Court play?**

The court will have a new civil process to provide a speedy, efficient and relatively cheap legal avenue for dealing with the most serious cases of cyber bullying.

The court's jurisdiction would cover all forms of electronic communication. This includes comments on websites, message boards, blogs and social media platforms, as well as emails and texts.

The distinguishing feature of electronic communication is its capacity to spread communications far beyond the original sender and recipient. Therefore the court's jurisdiction will not cover telephone calls, hard copy correspondence and in person behaviour.

### **Who can make a complaint to the District Court?**

The new approved agency is the first port of call for complainants.

If the approved agency cannot resolve the complaint (eg, the perpetrator refuses to engage or cannot be contacted), the complainant can then apply to the District Court for a civil order in relation to their case. Parents and school principals can apply on behalf of children in their school.

In addition, the Police will be able to apply to the court for a civil order where a communication constitutes a threat to a person's safety.

The Chief Coroner will be able to make an application to the court for a take-down order about material relating to suicide, if publication is prohibited by the Coroners Act 2006.

### **What will be the threshold for taking a civil case to court?**

Only serious cases that have already been considered by the approved agency should go before the court.

Complainants will be required to show that the communication is a serious or repeated breach of one of the communication principles and it has caused, or is likely to cause, serious emotional distress.

It is estimated that about 100 cases will come before the court each year.

## **What kinds of communications or information would the court take action against?**

The Bill adopts the 10 statutory principles recommended by the Law Commission, which are based on criminal and civil law and regulatory rules.

They include that a communication should not:

- disclose sensitive personal facts about an individual
- be threatening, intimidating, or menacing
- ☐ be grossly offensive to a reasonable person in the complainant's position
- incite or encourage anyone to send a message to a person with the intention of causing that person harm
- incite or encourage another person to commit suicide, or
- denigrate a person's colour, race, ethnic or national origins, gender, sexual orientation or disability.

The court will only make an order if there is a serious or repeated breach of at least one of the principles.

The court will also take into account people's right to freedom of expression, along with other relevant considerations, including:

- the content of the communication
- level of harm caused
- purpose of the communication (for example, humour is different from malice)
- extent to which it has spread
- age and vulnerability of a complainant
- truth or falsity of statements
- conduct of the defendant, including attempts to minimise harm, and
- conduct of the complainant.

## **What action will the court be able to take?**

The court will be able to order a broad range of remedies, including:

- orders to takedown material (issued against either the perpetrator, an ISP, a website host or any other relevant internet intermediary)
- cease-and-desist orders
- orders to publish a correction, an apology or give the complainant a right of reply
- ordering the release of the identity of the source of an anonymous communication, and
- ordering name suppression for any parties.

## **Will the court have the power to impose criminal or monetary sanctions?**

No. However, failure to comply with an order would be an offence punishable by a fine.

### **Could the court's rulings be appealed?**

Yes. An appeal of the whole or part of a decision can be made to the High Court. Any subsequent appeals on points of law would be made to higher courts.

### **How do the proposals affect people's freedom of speech rights?**

Section 14 of the New Zealand Bill of Rights Act 1990 guarantees the right to freedom of expression.

However, it is not an absolute right, and freedom of speech does not automatically trump offences and protections set out in other laws.

Therefore, the new proposals are consistent with the Bill of Rights Act.

Also, the District Court and the approved agency will have to act consistently with the Bill of Rights Act and consider the importance of freedom of expression when considering complaints, making decisions and issuing sanctions.

Clear criteria will be used to determine whether someone has broken the law. For example, the new communications offence would only apply where:

- the person sending the communication intended to cause serious emotional distress to a victim;
- the communication would cause serious emotional distress to an ordinary reasonable person in the position of the victim;
- the communication caused serious emotional distress to the victim

It will be up to the courts to decide when the line has been crossed, and anyone found guilty can appeal a decision, just as they can with any other kind of prosecution.

This will help protect people's free speech rights.

### **How will anonymous sources of harmful communications be dealt with?**

In some situations, victims might not know who is sending them messages or who is responsible for posts on websites or social networks.

Complainants can ask the approved agency to investigate. The agency could pass on a request for removal, modification or correction of the harmful communication to an internet service provider, or other appropriate internet entity such as Facebook, Twitter or Google.

If that does not address the situation, the court could order the internet intermediary to provide identity details. Once provided, the court would have discretion to determine whether or not to remove anonymity.

### **How will complaints against harmful communications posted on offshore-based websites and platforms be enforced?**

Many complaints relate to communications on large, popular, established sites and platforms.

Overall, it is expected that most court-ordered sanctions will be directed at specific individuals – the perpetrator of the harmful communication – who will often live in New Zealand. Even if the website or software they used is not New Zealand-based, such people could be fined or jailed if convicted.

In some circumstances, the court may make an order against an overseas-based website host, ISP or application service provider. There are few mechanisms to enforce such orders. All countries face this issue, which continues to change as technology evolves. The main solution is multilateral action and cooperation. This work is on-going.

As the Law Commission's report noted, large corporations like Google and Facebook have well developed protocols for responding to authoritative requests from governments and law enforcement agencies for information about users, or to notices and takedown orders.

Companies are also directly fronting up to cyber bullying. For example, Facebook has added an antibullying page to its Family Safety Center, with tools, tips and programmes to help people stand up for each other, and instructions on how to report a problem.

Additionally, when people need additional help, organisations such as NetSafe have a successful track record of liaising with internet companies and social networking platforms to resolve problems.

### **What costs are associated with the new regime?**

Some funding may be required for the approved agency under the new civil enforcement regime. Any costs will be finalised when decisions are made about setting up or appointing the agency.

There will be some costs (that is, court staff and judicial time) related to the District Court's role in the new civil enforcement regime. This will be absorbed in Ministry of Justice baselines.

Internet service providers or website hosts may face some minor additional compliance costs related to some measures, such as taking down material or identifying the account holder of an internet protocol (IP) address that is the source of the harmful communications.



However, any costs would be minor. Most companies already have relevant protocols and processes in place to deal with existing requests from law enforcement agencies. Also, NetSafe's submission to the Law Commission's issues paper noted that in around 90 percent of the complaints they receive, the victim knows the identity of the perpetrator.

### **What will be done to address cyber bullying in schools and by school-age children?**

Schools need to be able to use new technology for teaching and learning purposes and to help their students manage the rapidly changing social environment that comes with it. Cyber bullying is of increasing concern to schools, students and parents.

National Administration Guideline 5 requires Boards of Trustees to provide a safe physical and emotional environment. This includes addressing bullying (including cyber bullying). To assist Boards with their obligations and provide guidance for reporting serious incidents of bullying, the Ministry of Education is drafting a resource for National Administration Guideline 5. This will be provided to schools in the next few months.

Two recent programmes to assist schools to address bullying behaviour have been introduced:

Wellbeing@school and Positive Behaviour for Learning.

The Wellbeing@School website provides schools with self-review tools to build a safe and caring climate that deters bullying. More information is available at <http://www.wellbeingatschool.org.nz/>.

Positive Behaviour for Learning provides tools for schools, teachers and parents to help create a school environment that encourages positive behaviour and learning. More information is available at <http://pb4l.tki.org.nz/>.

Netsafe is contracted by the Ministry of Education to promote safe and responsible use of online technologies. Their information includes the use of information and communications technology contracts and provides a template. The Ministry will promote the contract to schools as good practice.