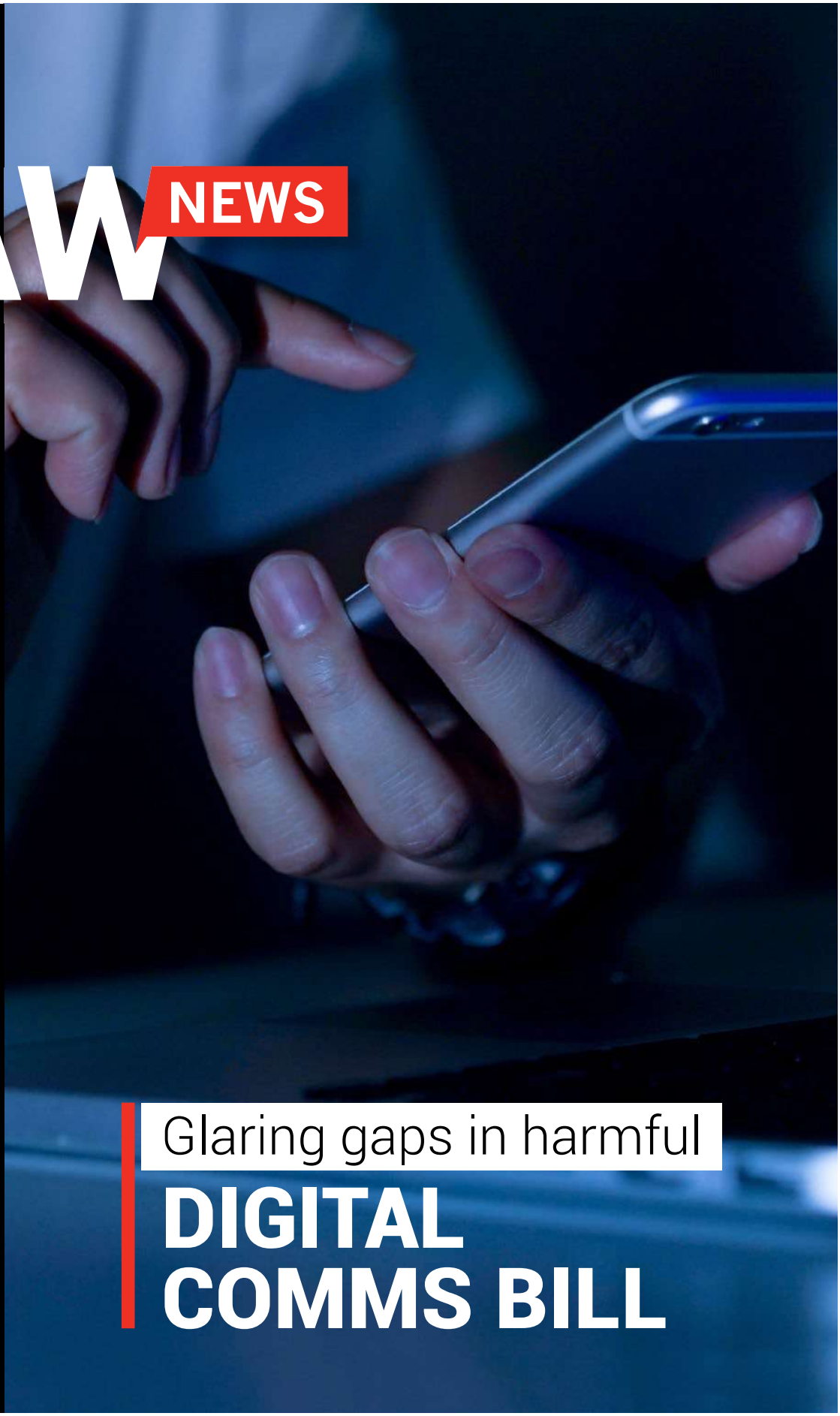
LAW NEWS

Nov 12, 2021
Issue 40

Inside



Glaring gaps in harmful

DIGITAL COMMS BILL

ADLS
adls.org.nz

Contents

Photo: Lorado / Getty Images

Hate speech law: balancing free speech with curbing terrorism

LAW NEWS

LawNews is an official publication of Auckland District Law Society Inc. (ADLS).

Editor: Jenni McManus
Publisher: ADLS

Editorial and contributor enquiries to:
Jenni McManus
021 971 598
Jenni.Mcmanus@adls.org.nz
Advertising enquiries to:
Darrell Denney
021 936 858
Darrell.Denney@adls.org.nz

All mail to:
ADLS, Level 4, Chancery Chambers, 2 Chancery Street, Auckland 1010
PO Box 58, Shortland Street DX CP24001, Auckland 1140, adls.org.nz

LawNews is published weekly (with the exception of a small period over the Christmas holiday break) and is available free of charge to members of ADLS, and available by subscription to non-members for $140 (plus GST) per year. **To subscribe, please email reception@adls.org.nz.**

Cover:
Chainarong Prasertthai / Getty Images

TECHNOLOGY AND THE LAW

A glaring gap in the harmful digital communications bill

People's lives have been destroyed and I've found myself standing in front of judges who are asking me why the police are not acting on the matter with no answer that I can give them

Rod Vaughan

Lawyers and victim advocates welcome the proposed amendments to the Harmful Digital Communications Act (HDCA) but say they do not go far enough and fall short of providing victims with a quick and efficient means of redress.

The Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Bill 2020 is awaiting its second reading in the House. Introduced by Labour MP Louisa Wall, the bill removes the need for the police to prove a perpetrator intended to cause serious harm and makes it an offence to share intimate visual recordings of another without express consent.

But a glaring omission from the bill is its failure to deal with deepfakes – highly doctored images or videos of people in compromising situations that are so realistic that they appear to be genuine.

Deepfakes are one of the most pernicious and distressing forms of cyber-bullying, yet the new bill offers no protection for victims.

Fake images have been around for as long as photography and film have existed but state-of-the-art digital technology has taken them to a new level.

They first came to prominence in 2017 with the sharing of pornographic videos that appeared to feature popular female celebrities. Within two years, almost 15,000 deepfakes were circulating online, most of them pornographic and featuring female celebrities.

Arran Hunt, a partner at Stace Hammond and a member of the ADLS Technology and Law committee, says he is deeply concerned that deepfakes are not covered by the new bill.

"Such technology is now available without cost to anyone who owns a smartphone," he says. "Utilising several generic photos of someone from social media, they can quickly be inserted into any manner of video or images, including ones that once released are likely to cause serious emotional distress.

"It won't matter that it wasn't actually them and that the video has been faked. It will have the same effect as genuine intimate visual material and would be posted with the same purpose in mind – to cause harm.

"This is why we believe that the bill should be updated to clarify that the definition of 'made' includes deepfakes.

"Without such an alteration, people creating and posting deepfakes will not automatically be caught by the Act and may have a good defence in that the videos may not strictly meet the definition of intimate visual recording."

Barrister Kathryn Dalziel is another who believes deepfakes should be included in the amended legislation.

"This type of artificial but entirely realistic image wasn't contemplated at the time the Act came into force and does not address where people suffer harm at having such believable images circulated about them.

"This is an omission in the Act and should be properly addressed to ensure that the offence targets abusive use of synthetic media and does not impact on legitimate audio-visual effects applied to imagery."

Arran Hunt

Kathryn Dalziel

Perceived deficiencies

The Harmful Digital Communications Act was introduced by National in 2015. It covered a wide range of offending such as online and mobile communications used to send or publish threatening or offensive material and messages, spread damaging or degrading rumours or publish invasive or distressing photographs or videos.

It incorporated criminal and civil offences to be handled by the police and Netsafe respectively.

According to the Ministry of Justice, there were 270 convictions under the Act between 2015 and 2020 while a Netsafe survey in 2019 found 5% of New Zealand adults – 170,000 people – had been the victim of online image-based abuse. Women made up 95% of the victims.

The Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Bill 2020 has been introduced to remedy some of the perceived short-comings of the Act.

This bill is designed to clarify the Act as it relates to intimate visual recordings by:

- making it an offence to share an intimate visual recording of another person without their express consent;
- imposing a penalty of up to three years' imprisonment, or a

Continued on page 04

Continued from page 03

fine of up to $50,000, for an individual convicted of this offence or, for a company, a fine of up to $200,000; and

- allowing the courts to issue orders to remove or disable intimate recordings that have been shared without consent.

The current Act requires proof of intent to cause harm for a digital communication to be considered an offence and the victim must have experienced a certain level of harm.

The Bill removes this test in the case of intimate visual recordings, so unauthorised sharing of this content would be an offence regardless of the level of harm that was intended or caused.

Hunt says the 2015 Act was flawed from the beginning.

"The original Law Commission suggestion was for a civil process that allowed for a 'quick and efficient means of redress' as is mentioned in s 3 of the Act. However, the government at the time introduced only half of the Law Commission's suggestion.

"It removed the part that was there to make it quick and efficient. Instead, they left it to the courts to interpret what 'quick and efficient' meant and, for courts, that means following the traditional process."

Hunt says this may not be an issue for matters that meet the criminal threshold as the police have the funding and experience to handle such a process.

"The criminal threshold comes down to the intent of the communicator, whether it was done with the intention to cause harm. But where it doesn't meet the criminal threshold, it's left to the parties to go through the usual slow court process.

"At that point it often comes down to the applicant not having the funds to undertake that process or going through a drawn-out process that can add to the harm."

Police inaction

Hunt says court orders that may be needed to search social media accounts offshore can cost around $1,000 each.

"We have contacts with several of the social media companies now so can sometimes facilitate service without that process, but for most that cost of service alone will stop them proceeding.

"If a victim can't afford to pay for that, they typically won't be able to afford a lawyer, leaving them either unrepresented, or our firm acting *pro bono*.

"And if the respondent is identified and defends it, then it can become a battle of attrition."

Hunt says he's been involved in matters which have had weeks in court at great cost to both sides.

"This is not a quick and efficient means of redress. It's a fight to push the other to the verge of bankruptcy. And they are fighting just to have a court tell someone to stop posting. That's really about the limit of the court's power. So high costs, but for very little."

Hunt supports the government's proposed amendments to the Act which seek to have some civil matters handled in the same way as criminal cases and to force the police to act on crimes.

Ruth Money

Martin Cocker

Court orders that may be needed to search social media accounts offshore can cost around $1,000 each

"In the past, they have been reluctant to take any action, as has the minister. There should be an expectation that to post someone's intimate visual recordings without consent will cause them harm. We believe that most people would probably already think that way.

"However, we've had several clients who have been told the opposite by the police.

"One client had photos and videos of herself posted to social media on more than one occasion without her consent or knowledge of who was posting them.

"But when she initially went to the police, she was told that as she had given an ex-partner the photos and videos, it was her own fault, and they wouldn't take action.

"Letters to the police officer involved went unanswered, as was our initial letter to the Minister of Police. He bothered to respond only after another MP raised it with him, but even then it went nowhere."

Hunt says yet another client had videos taken by a professional photographer who uploaded them to pornography websites without her consent.

"Again, the police refused to act, claiming that she had somehow given non-verbal consent to those videos being published publicly. The police admitted there was no verbal or written consent but just assumed that consent was given.

"People's lives have been destroyed and I've found myself standing in front of judges who are asking me why the police are not acting on the matter with no answer that I can give them.

"The police have taken a path that prevents victims from gaining the access they deserve, leaving them to seek civil action."

Revenge porn

Dalziel says the Act needs improvements to help victims make their case and is concerned that the threshold is too high for so-called revenge porn.

"For the offence of causing harm by positing a digital communication, it has to be established that the person posting a digital communication intended to cause serious emotional distress (harm) to a victim.

"The threshold is too high for instances where there has been a relationship breakup and intimate visual recordings made during that relationship are posted online for the purposes of causing some emotional distress but are not posted with the intention to cause serious emotional distress," she says.

"The Act should not have required 'serious' emotional distress or included an objective test in respect of a subject person's emotional distress.

"The amendment is important because revenge porn is prevalent and sexually abusive. It involves sharing of very private information with people for whom the pictures were not intended

Continued on page 04

Photo: Peter Dazeley / Getty Images

Continued from page 04

in what can be a very public way."

Dalziel says the images can stay online forever unless there is an order requiring them to be taken down.

"By then, the images may have circulated into environments where the victim has no knowledge and therefore cannot control access to the images. It causes humiliation, embarrassment and trauma for victims."

Wrong agency?

Victim advocate Ruth Money, who has assisted victims of crime on a voluntary basis for almost a decade, believes the amendments to the bill will only be as effective as the two agencies approved to assess complaints – the police and Netsafe.

But she says it's of immense concern that the performance of Netsafe, which has assisted more than 14,000 people since 2016, "is beyond woeful".

"In fact, in many instances they have caused additional harm to the already harmed and vulnerable survivors. In my personal experience and [the] experience of many, many other survivors, Netsafe is not the appropriate agency to hold this important position."

Money contends that Netsafe is not adequately trained, its management does not understand sexual violence and it fails to undertake investigations.

"They simply do not investigate, which is a core function under the Act," she says. "It is my experience and that of others that they make subjective judgments, perpetuate harm, enable abusers to continue to engage and control their victims, supply incorrect information (ACC referrals, for example) and leave survivors in a worse state than they were when they first contacted them."

Money believes the correct agency should be a specialist division of the police.

"Netsafe's role and efficacy, specifically regarding HDCA complaints, should be independently reviewed and moved to NZ Police urgently, given its importance to ensure the legislation works for those who have been harmed.

The current Act requires proof of intent to cause harm for a digital communication to be considered an offence and the victim must have experienced a certain level of harm

"Currently police are confused by Netsafe's role versus their own and this structure has caused a 'no-man's land' where survivors are lost and further harmed.

"Netsafe may well be qualified to teach people about online scams and educate children about staying safe online, but an investigative and trauma-informed agency to assist victims of sexual abuse they most certainly are not.

"This is a specialist role that requires skilled professionals," she says.

Her assertions are endorsed by Hunt who says a specialist division of the police may be a better option than Netsafe as long as they are well trained.

"So far, we haven't often seen the police take such matters as seriously as they should or with consideration of the amount of harm being caused.

"However, trained officers could better understand the harm that such communication can cause and can take an approach that would minimise future harm caused by the victims.

"To be fair to them, we can't expect Netsafe to act like a police force. Their job isn't to say what is criminal and what is civil. However, I can see Ms Money's point as to whether they are suitable.

"Correctly trained, police may be a better option, replacing Netsafe's role, but that would still require a significant change to the Act. I don't believe that just replacing Netsafe with the police would solve the issues, as it would still leave many to the perils, and added harm, of the inefficient process.

"An updated Act utilising specially trained police and with an efficient process would be better for all parties involved."

For his part, Netsafe chief executive Martin Cocker says last year it received more than 4000 requests for assistance in its role as approved agency under the Harmful Digital Communications Act.

"Approximately 1% of those people have then chosen to progress on to the District Court. The average customer satisfaction for this service in the last quarter was 8.4 out of 10. So, in terms of filtering out matters – and the general role of the approved agency under the act – the process is working.

Cocker says such results have been achieved because Netsafe is not a regulator or enforcement agency but resolves complaints through the use of advice, negotiation, mediation and, where appropriate, persuasion.

"But that also places limitations on what we can do. This Netsafe process is useful as part of a mix of services to assist victims of sexual violence but should not be the primary response.

"Equally, as an online safety agency, Netsafe should not be the primary response agency on matters of sexual violence."

Cocker says as the volume and complexity of online safety incidents continue to grow, it is reasonable to ask whether any one agency and process can effectively serve all those cases.

"It is certainly foreseeable that in the coming years the role that Netsafe and the police play will be spread across multiple agencies providing more specialist services for specific harm types." ■