Women and Technology

By Justice Susan Glazebrook[1]

Technology is a feature of modern life and it will no doubt become more and more important in our lives and those of our children. There are many ways in which it has changed our lives for the better. It does, however, have its dangers. For example, the same 3D printing technology that enables an amputated limb to be replaced quickly and cheaply can also be used to produce a weapon. Drones can transport life-saving blood to accidents, but they can also breach privacy rights, endanger aircraft and fire weapons.[2] Artificial intelligence can be used to diagnose illnesses. But on the other hand, it can also exacerbate bias and inequality. For instance, Amazon had to abandon an algorithm it was using to sort job applicants because it only selected male candidates.[3] This was because for its dataset, the algorithm used the CVs of candidates over the previous ten years – which consisted predominantly of male candidates.

The New Zealand Government has recognised the need for safeguards when using algorithms in government decision making in a report published by Statistics New Zealand. This report recommended safeguards for their use, including that government departments and agencies must demonstrate clear public benefit from using an algorithm, recognise the possibility of bias and provide for ultimate human supervision and override.[4] As a result of this report, the Algorithm Charter was instituted which has a number of Government departments as signatories.[5] The intent of the charter is to ensure "New Zealanders have confidence in how government agencies use algorithms" and as a means of providing public accountability. The guiding principles of the Charter are transparency, partnership,[6] people, data, ethics and

---

1 Judge of the Supreme Court of New Zealand. This paper elaborates on a speech given at the International Association of Women Judges (IAWJ) Asia-Pacific Regional Conference in Bohol on 28 February 2019. My thanks to Rachel McConnell, Rebecca McMenamin and Don Lye for their invaluable assistance.

2 Australian Human Rights Commission *Human Rights and Technology Issues Paper* (July 2018) at 7.

3 James Cook "Amazon scraps 'sexist AI' recruiting tool that showed bias against women" *The Telegraph* (online ed, London, 10 October 2018); and Reuters "Amazon ditched AI recruiting tool that favored men for technical jobs" *The Guardian* (online ed, London, 11 October 2018).

4 Stats New Zealand *Algorithm Assessment Report* (October 2018). The report surveyed 12 major New Zealand Government departments about their use of algorithms, such as the Ministry of Justice, the New Zealand Police, the Ministry of Education and the Ministry of Health. See 37–38 of the report for a list of the agencies and the algorithms used

5 New Zealand Government *Algorithm Charter for Aotearoa New Zealand* (July 2020).

6 Partnership is regarded as one of the principles of Te Tiriti o Waitangi/the Treaty of Waitangi. Any algorithm used must be consistent with the Treaty.

oversight.[7] Part of the framework is that algorithms are regularly reviewed and there is active engagement with those who may be greatest impacted by their use."

Perhaps the most visible way technology has transformed our lives is through the internet. Thanks to social media, we now have an unprecedented number of ways to keep in touch with friends and families, even if they are based in different countries. Access to the internet and mobile phones has also transformed the lives of many women: from allowing them to receive an education[8] to gaining access to health services[9] and developing businesses.[10] Social media and the internet have also allowed greater global co-ordination around social issues. I mention, for example, the #MeToo movement.[11] And consumers are more and more able to put pressure on companies by taking concerted action to confront issues on social media.[12]

On the negative side, every time someone uses the internet or social media, they leave a digital footprint. Privacy International has reported that medical apps, such as those that monitor heartrates, menstrual and fertility cycles, share data with Facebook which can then tailor advertisements based on the results.[13] Most damningly, it also found that 'opting out' through the app or Facebook settings made no difference to the information being shared.[14] To add to the difficulty, users will often not know what information companies are collecting, how they are collecting it and what they are collecting it for. The terms and conditions of use tend to be

---

7 Algorithm Charter, above n 5, at 3.

8 Intel Corporation *Women and the Web* (2012) at 30–32. Intel conducted a survey into women's access and use of the internet. Most of the respondents reported they used the internet primarily for their own education.

9 For example, automated voice messages containing vital health information are sent to pregnant women in Ghana. See Elie Chachoua "How mobile technology could change healthcare in developing countries" (18 March 2015) World Economic Forum <www.weforum.org>. Many women also report using the internet to research health information: Intel Corporation, above n 8, at 32.

10 For example, Soko is an online shopping site which sells items from artisans in developing countries, <shopsoko.com>..

11 The #MeToo movement went viral in October 2017 as a result of allegations by many actresses of sexual abuse by Harvey Weinstein (a Hollywood producer). Alyssa Milano (a US actress) urged her followers on Twitter to tweet #MeToo if they had been sexually harassed or assaulted to show the magnitude of the problem.

12 For example, in 2010, Greenpeace initiated a social media campaign against Nestlé for their use of unsustainably sourced palm oil. Thousands of protestors participated in the campaign on Facebook and Twitter. As a result, Nestlé agreed to stop using palm oil produced by Sinar Mas, a company which Greenpeace had criticised for rainforest deforestation. HSBC also agreed to sell its shares in Sinar Mas. See Lucie Harrild "Lessons from the palm oil showdown" *The Guardian* (online ed, London, 27 October 2010); and Emily Steel "Nestlé Takes a Beating on Social-Media Sites: Greenpeace Coordinates Protests Over Food Giant's Palm-Oil Purchases" *The Wall Street Journal* (online ed, New York, 29 March 2010).

13 Privacy International *How Apps on Android Share Data with Facebook* (, December 2018) at 4.

14 At 4.

lengthy and written in legalese, making it unlikely that they are even read, let alone understood.[15]

I now turn to the benefits and dangers of technology with regard to violence and harassment directed against women and children, mostly in a domestic violence context. I have divided my remarks into the good, the bad and the even worse.

I start with the good

In New Zealand, technology has been utilised to help keep women and children safe after incidents of domestic violence. When attending the scene of domestic violence incidents, the New Zealand police use two algorithms that assess the risk of future offending.[16] This helps them decide on an appropriate response, both for the immediate situation and for later measures, such as ongoing protection for the victims or prosecution decisions. The tools support, but do not replace, human judgement in situations that can be complex and challenging.

More generally, technology enables women and children to keep in touch with support networks of friends and families. There are also women-focused apps available that allow women to manage their safety,[17] including women-only ride shares.[18] Electronic tracking can also protect victims while offenders or alleged offenders are out on bail or parole or subject to conditions of restraining or protection orders.[19]

---

15 To illustrate the point, a journalist spent seven days in an experiment to see how long it would take to read the terms and conditions of 33 companies: Alex Hern "I read all the small print on the internet and it made me want to die" *The Guardian* (online ed, London, 15 July 2015). An experiment conducted by communications professors from York University (Toronto) and the University of Connecticut also found that three-quarters of participants did not read the terms and conditions when they were asked to join a fictitious networking site: Jonathan A Obar and Anne Oeldorf-Hirsch "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services" (2020) 23 iCS 128.

16 The two algorithms are the Static Risk algorithm and the Dynamic Risk Measure algorithm. The Static Risk algorithm calculates the probability that a family violence perpetrator will commit a crime against a family member within the next two years using police data such as gender, past incidents of family harm, and criminal history. The Dynamic Risk Measure algorithm makes an assessment based on the current circumstances against a range of safety concerns: Statistics New Zealand, above n 4, at 20.

17 For example, the Bsafe app that has allows you to select "guardians" who receive an alert and a livestream of your location if the SOS button is set off: "Bsafe" <www.getbsafe.com>.

18 Such as "Safr": <www.gosafr.com>; and "Shebah": <www.shebah.com.au>.

19 Electronic monitoring is available in New Zealand for selected defendants on bail (EM bail): Department of Corrections "Electronic Monitoring on Bail (EM bail)" (17 November 2020) <www.corrections.govt.nz>. Electronic monitoring can also be a condition of release by the Parole Board: Parole Act 2002, s 15(3)(f).

The New Zealand Police are also increasingly taking video statements from victims at the scene or soon after.[20] This ensures that victims provide a first-hand account in their own words while their memory is fresh. Such video interviews may be admissible in evidence in court, even if later victims decide they do not wish to pursue the case or retract their evidence.[21]

Video interviews have become the norm for child victims in New Zealand. Such interviews are conducted as soon as possible after the alleged offending and by specialist interviewers in child-friendly environments.[22] These interviews are admissible as evidence-in-chief in court.[23] Any further questions can also be asked in court through audiovisual links to ease the pressures of the court process on victims.[24]

Technology has also made getting help for domestic violence easier, with the internet providing links to resources for victims. Some New Zealand businesses now host "Shielded Sites" which, in addition to their regular business functions, also provide domestic violence victims a clickable button to get help which does not get logged into the browser history.[25] Many also have 'quick hide' buttons that divert the page to news websites should a perpetrator approach while victims are using a computer to seek help.[26]

Now to the bad

Abusers have been enabled by social media and the internet to carry out cyber abuse and harassment, often with impunity. This can consist of bombarding a victim with text messages

---

20 See New Zealand Police *Victim Video Statements (VVS): User Guide* (March 2020) (Obtained under Official Information Act 1982 Request to the New Zealand Police).

21 Family violence victims may retract their statement under coercion or self-preservation: See Susan Glazebrook "Family Violence – domestic measures for a global problem" (13 May 2015) Courts of New Zealand <www.courtsofnz.govt.nz> at 26–27. Section 18 of the Evidence Act 2006 provides that hearsay can be admissible, provided the circumstances under which the statement was made indicates its reliability and that the person who is making the statement is "unavailable" as a witness.

22 Oranga Tamariki "Specialist child interviews" (11 October 2021) <practice.orangatamariki.govt.nz>. In New Zealand, children who may be victims of abuse are interviewed by a specialist child interviewer at specialist video interview units which provide a safe, non-threatening environment. The New Zealand Police also has its own guidelines for conducting interviews with child witnesses: New Zealand Police *Specialist Child Witness Interview Guide* (1 November 2016) (Obtained Under Official Information Act 1982 Request to the New Zealand Police).

23 Evidence Act, s 107.

24 See generally Courts (Remote Participation) Act 2010. After a successful pilot, specialist Sexual Violence Courts were made permanent (although only running out of Auckland and Whangārei). These courts use technology to lessen the impact on victims giving evidence in Court. Within these courts, the judge actively enquires about the mode of evidence preference (compared to the normal process of having to make a formal application for an alternative method of giving evidence). The default position within the Sexual Violence courts is that examination will be conducted via CCTV: see Sue Allison and Tania Byer *Evaluation of the Sexual Violence Court Pilot* (Ministry of Justice, June 2019) at 5.3.

25 See "The Shielded Site Project" <www.shielded.co.nz>.

26 For example, "Are you OK" <www.areyouok.org.nz>.

and voicemails. Other types of abuse include so-called revenge porn and posting information on social media with a view to causing embarrassment or humiliation.

Technology has also greatly enhanced the methods available to domestic abusers who exercise coercive control over their victims. This type of abuse involves a pattern of behaviour where the abuser utilises intimidation, often paired with physical victimisation, to create dependence, isolation and a climate of fear.[27]

With technology the abuser can be ever present even after the relationship has ended. There is now, for example, the ability to monitor from a distance through tracking use of email accounts, banking passwords, spyware and monitoring browsing histories. As an example in Australia, an ex-partner found out the location of a women's refuge centre after he put a tracking device in his daughter's doll at an access handover.[28] In another example from the US, a stalker tricked an ex-partner into installing spyware onto her computer by sending her an email, which upon being opened, automatically installed the spyware onto her computer without any notification.[29]

And now I turn to the even worse

I deal in this section with issues related to cyber bullying and harassment of children, as well as the issue of self-harm. I characterise these issues as even worse because they involve children, who are our future and who should be protected from avoidable harm, while of course being left the freedom to develop their own lives as they would wish.

Children now often have access to the internet through personal devices which means less supervision over content accessed and over their interactions with others. This makes it harder to protect them. There have been several high-profile cases globally of young people committing suicide as a result of cyber bullying. In 2015, UK teenager Ronan Hughes committed suicide after being blackmailed by scammers who had tricked him into sharing intimate pictures that were then shared with his friends when he failed to pay the ransom.[30]

---

27 See generally Julia Tolmie and others "Social Entrapment: A Realistic Understanding of the Criminal Offending of Primary Victims of Intimate Partner Violence" [2018] NZ L Rev 181.

28 Matt Wordsworth "'Stalker apps' and GPS allow domestic violence abusers to discover hidden refuges" (28 June 2015) ABC News <www.abc.net.au>.

29 Cynthia Fraser and others "The New Age of Stalking: Technological Implications for Stalking" (2010) 61(4) Juv & Fam Court J 39 at 46.

30 Aaron Rogan "Schools will warn pupils of online 'sextortion'" *The Times* (online ed, London, 6 February 2019).

There is also concern about young people accessing sites which glorify self-harm and eating disorders. While the terms of use usually set a minimum age, the inability of sites to verify age means that many children are able to access these sites. Thirty families in the UK have accused social media companies of aiding their children's suicides by hosting pro-suicide content on their sites, including images of self-harm.[31] In a recent UK case, teenager Molly Russell's account continued to receive pro self-harm content even after her suicide. These posts continued due to algorithms that suggest content based on previous activity.[32]

So what can be done?

First, many of these behaviours are covered to some extent by existing legislation, including criminal legislation and domestic violence legislation.[33] But this legislation has its limitations, often because online abuse was not in contemplation when the legislation was passed. Some jurisdictions, including New Zealand, do have some specialist legislation dealing with certain types of cyber abuse[34] but this legislation often still has limitations.[35] One of the issues is the fact that internet providers and content hosting sites are often located offshore and are essentially self regulating. Thus far, the technology involved and social media business models have been insufficiently understood outside of the technology sector to be regulated appropriately.[36] This is likely due to the speed at which technology has developed and the treatment of algorithms as trade secrets.

In the past, the view has been that social media companies are not publishers but were merely platforms for sharing content, thus bearing no responsibility for dangerous content hosted on

---

31 Sian Griffiths, Rosamund Urwin and Caroline Wheeler "Revealed: how Big Tech pushes teens like Molly Russell to suicide" *The Times* (online ed, London, 27 January 2019).

32 Rosamund Urwin and Sian Griffiths "Pinterest emailed suicide tips after Molly Russell's death" *The Times* (online ed, London, 27 January 2019). Some four years after her death, her inquest has been delayed because of the failure to get full disclosure of information from social media giants: see BBC News "Molly Russell: Social media users 'at risk' over self-harm inquest delay" (8 February 2021) <www.bbc.com>. After a number of pre-hearings, the inquest is due to take place in April 2022: Tom Knowles "Molly Russell coroner calls for safer internet" *The Times* (online ed, London, 7 December 2021).

33 For example, Harassment Act 1997 and the Domestic Violence Act 1995.

34 For example, Harmful Digital Communications Act 2015.

35 See Ruby King's critique on the Harmful Digital Communications Act 2015 and the Harassment Act 1997: Ruby King "Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation?" (2017) 48 VUWLR 29.

36 For a comprehensive treatment of this topic, see John Armour and others "Putting technology to good use for society: the role of corporate, competition and tax law" (2018) 6(1) Journal of the British Academy 285.

their websites.[37] Although social media companies are now starting to try and control content this is still largely at their discretion and using their views on what is appropriate or not. Facebook, for example, has faced criticism for taking down sites promoting breast feeding or showing pride after breast cancer surgery, while leaving intact very damaging material.[38]

Some commentators have suggested that radical reforms are needed. One suggestion was that there should be a total ban on certain content and that companies should have strict liability for harm.[39] It was suggested that this be paired with requiring public disclosure of legal compliance, personal liability for CEOs or managers and a longer vesting period for managerial compensation.[40]

A green paper was released in the UK in 2017 regarding internet safety and the types of harm it can cause.[41] The paper established three key principles:[42]

(a) What is unacceptable offline should be unacceptable online;

(b) All users should be empowered to manage online risks and stay safe; and

(c) Technology companies have a responsibility to their users.

The UK is also currently considering several legislative provisions to enforce corporate responsibility onto social media giants.[43] These include the establishment of a regulatory body; fines up to 17.5 million pounds; corporate manslaughter charges; and personal criminal liability for CEOs.[44] The Online Safety Bill is still in its draft phase but its coverage is broad. It seeks

---

37 Sam Levin "Is Facebook a publisher? In public it says no, but in court it says yes" *The Guardian* (online ed, London, 3 July 2018).

38 Facebook moderators are provided with internal training manuals and flowcharts in making decisions on what content to remove: Nick Hopkins "Revealed: Facebook's internal rulebook on sex, terrorism and violence" *The Guardian* (online ed, London, 21 May 2017. For example, adult nudity in the context of the Holocaust is acceptable but not child nudity. There was controversy over Facebook's removal of the famous 'napalm girl' Vietnam war image, although Facebook later backed down: Sam Levin "Facebook backs down from 'napalm girl' censorship and reinstates photo" *The Guardian* (online ed, London, 9 September 2016).

39 Armour and others, above n 36, at 294.

40 At 298–300.

41 HM Government *Internet Safety Strategy – Green paper* (October 2017).

42 At 3.

43 See generally Secretary of State for Digital, Culture, Media & Sport and Secretary of State for the Home Department *Online Harms White Paper* (CP 57, April 2019); and the consultation outcome Secretary of State for Digital, Culture, Media & Sport and Secretary of State for the Home Department *Online Harms White Paper: Full Government Response to the Consultation* (CP 354, December 2020).

44 Ryan Browne "Social media giants face big fines and blocked sites under new UK rules on harmful content" (15 December 2020) CNBC <www.cnbc.com>.

to impose duties of care on providers of user to user services.[45] It has three aims: to prevent illegal content online, to protect children from harmful material and to protect adults from legal but harmful content.[46] Providers are obliged to carry out risk assessments on content both to children and adults.[47]

The Bill has been criticised for not going far enough.[48] In its Select Committee process, further recommendations were made, including a restructure of the Bill completely as in its current format it is too complex.[49] The Committee also noted there was no clarity about what the legislation seeks to achieve.[50] Another recommendation was in relation to tackling foreseeable harm – such as auto-play features, the use of algorithms promoting content and geolocation data remaining on uploaded photographs, potentially providing locational data for those who are subject to family violence.[51] User to user services who fail to comply with the legislation "face fines of up to 18 million pounds or 10 per cent of their annual income, whichever is greater.[52]

Another measure increasingly being taken is the establishment of specialised tribunals or agencies to mitigate and educate about online harm. With the proposed Online Safety Bill in the UK, The Office of Communications (OFCOM) will be the body overseeing the legislation.[53] It will have wide enforcement powers, including the power to compel user to user services to attend an interview with them,[54] the ability to impose fines, enforcements actions and penalty notices.[55] The Select Committee also recommended that OFCOM be given even greater powers.[56]

---

45 Defined as any online service which allows users to share and upload content: Draft Online Safety Bill 2021 (CP 405) (UK), cl 2(1).

46 BBC News "Online Safety Bill: New offences and tighter rules" (14 December 2021) <www.bbc.com>.

47 Draft Online Safety Bill, cl 19.

48 Dan Milmo "MPs call for online safety bill overhaul to protect children and penalise tech firms" *The Guardian* (online ed, London, 14 December 2021).

49 Joint Committee on the Draft Online Safety Bill *Draft Online Safety Bill Report of Session 2021-2022* (HL Paper 129, HC 609, 14 December 2021) at 136.

50 At 136.

51 At 137–138.

52 Draft Online Safety Bill, cl 85.

53 OFCOM more generally is the agency that oversees all telecommunications and broadcasting standards in the UK.

54 Draft Online Safety Bill, cl 76.

55 Clause 90.

56 Joint Committee on the Draft Online Safety Bill, above n 49, at 150–157.

Education is also going to play a large part in reforming the internet. "Internet Legends" is a Google developed game used throughout UK primary schools to educate on internet safety.[57] New Zealand also has its own school programme run by NetSafe.[58] In New Zealand, NetSafe is the agency established to receive complaints and provide assistance around misuse of the internet.[59]

So to conclude

Technology has not caused many of the issues I have discussed but it has certainly exacerbated them. Measures to protect victims and hold abusers to account, coupled with proper regulation and corporate responsibility on the part of tech companies, will assist in mitigating the harm and giving redress to victims. However, societal change is needed to eliminate, or at least diminish, the underlying behaviours.

57 "Internet Legends" <beinternetlegends.withgoogle.com>.
58 "Netsafe Schools" < www.netsafe.org.nz>.
59 "About Netsafe" <www.netsafe.org.nz>.