MODELS OF CYBER HARASSMENT LAWS AND RELATED LEGISLATION

Comparative legal review of harassment and sexual exploitation laws across the Commonwealth
Outline

The Legal Assistance Centre and Sisters For Change have compiled four separate volumes of appendices to accompany the EJA report, *Comparative legal review of harassment and sexual exploitation laws across the Commonwealth*. The appendices are available in PDF format and provide excerpts of legislation on discrimination, harassment and sexual exploitation from across the regions of the Commonwealth, as well as relevant international and regional conventions and directives.

Appendix 2 Models of cyber harassment laws and related legislation includes excerpts of laws on online harassment and cybercrimes, voyeurism and laws on jurisdiction for the investigation and prosecution of cybercrimes from across the regions of the Commonwealth – Africa, Asia, Caribbean and the Americas, Europe and Pacific – as well as international conventions on violence against women and child sexual exploitation and abuse.

About Legal Assistance Centre

The Legal Assistance Centre (LAC) is a public interest law centre in Namibia which strives to make the law accessible to those with the least access, through education, law reform, research, litigation, legal advice, representation and lobbying, with the ultimate aim of creating and maintaining a human rights culture in Namibia.

About Sisters For Change

Sisters For Change (SFC) is an international NGO working to eliminate discrimination and violence against women and girls worldwide through legal reform, legal empowerment, legal accountability and legal advocacy strategies. SFC works to generate systemic change in how governments combat violence, structural change to give women voice and agency in justice systems and social change to end the social acceptance of violence against women and girls. SFC is active in the UK, India and Indonesia. As a member of the Equality & Justice Alliance, SFC is working to reform laws that discriminate against women and girls and LGBT people across the Commonwealth. SFC is currently working with the Governments of Namibia, Saint Lucia and Samoa on technical assistance programmes and is a member of the SADC Parliamentary Forum’s Technical Working Group on the development of a Model Law on Gender-Based Violence.

For more information visit

[www.sistersforchange.org.uk](http://www.sistersforchange.org.uk)

Follow us on @sisters_4change

Registered Company No. 9136425

Registered Charity No. 1165647

Copyright © Sisters For Change 2020

This work can be copied, shared and distributed, in whole or in part, for research, educational and public policy purposes subject to the condition that the work is not altered or adapted and the Equality & Justice Alliance is acknowledged as author of the work.

This work has been commissioned by Sisters For Change, a member of the Equality & Justice Alliance, but it has not been approved by, nor does it represent the opinions of, any other member of the Alliance.

Design by Bright Design, elaine_craig@hotmail.com

Sisters For Change is grateful to the UK Government Foreign & Commonwealth Office for supporting the work of the Equality & Justice Alliance.
# Contents

## A. Laws on online harassment and cyber crimes

| 06 | Commonwealth Africa |
| 06 | Botswana |
| 08 | Namibia |
| 11 | South Africa |
| 15 | Tanzania |
| 16 | Uganda |
| 17 | Zimbabwe |
| 18 | Commonwealth Asia |
| 18 | Singapore |
| 25 | Commonwealth Caribbean and Americas |
| 25 | Canada: Nova Scotia |
| 28 | Commonwealth Europe |
| 28 | United Kingdom: England & Wales |
| 30 | Commonwealth Pacific |
| 30 | Australia: Queensland |
| 32 | Australia: New South Wales |
| 35 | New Zealand |
| 40 | United States of America |
| 42 | International & Regional Conventions |
| 42 | African Union Convention on Cyber Security and Personal Data Protection 2014 |
| 43 | SADC Model Law on Computer Crime and Cybercrime 2013 |

## B. Related legislation: Voyeurism

| 45 | Commonwealth Pacific |
| 45 | Australia: New South Wales |
| 47 | Commonwealth Caribbean and Americas |
| 47 | Canada: Federal legislation |
| 50 | Commonwealth Asia |
| 50 | India |
| 51 | Commonwealth Europe |
| 51 | United Kingdom: England & Wales |

## C. Jurisdiction

| 53 | Commonwealth Africa |
| 53 | Botswana |
| 54 | Namibia |
| 54 | South Africa |
| 55 | Tanzania |
| 56 | Uganda |
| 56 | Zimbabwe |
| 57 | Commonwealth Asia |
| 57 | Singapore |
| 58 | International & Regional Conventions |
| 58 | Budapest Convention 2001 |
| 60 | Lanzarote Convention 2007 |
| 60 | Istanbul Convention 2011 |
| 61 | EU Directive 2011/92/EU |
| 61 | SADC Protocol on Mutual Legal Assistance in Criminal Matters 2002 |
| 61 | SADC Model Law on Computer Crime and Cybercrime 2013 |
Focus of review

1. Australia  Population of 25,499,884
2. Botswana  Population of 2,303,697
3. Canada  Population of 37,742,154
4. India  Population of 1,366,417,754
5. Namibia  Population of 2,494,530
6. New Zealand  Population of 4,822,233
7. Singapore  Population of 5,850,342
8. South Africa  Population of 58,558,270
9. Tanzania  Population of 58,005,463
10. Uganda  Population of 45,741,007
11. United Kingdom  Population of 67,530,172
12. United States of America  Population of 331,002,651
13. Zimbabwe  Population of 14,862,924
Models of cyber harassment laws and related legislation

- Singapore
- Australia
- South Africa
- Tanzania
- Namibia
- Botswana
- India
- New Zealand
- Uganda
- Zimbabwe
- Namibia
- India
- Singapore
- New Zealand
A. Legislation on online harassment and cyber crimes

Commonwealth Africa

BOTSWANA

Cybercrime and Computer Related Crimes Act 2018

14. Cyber extortion
A person who performs or threatens to perform any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by-
(a) undertaking to cease or desist from such actions; or
(b) undertaking to restore any damage caused as a result of those actions, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding 10 years, or to both.

16. Cyber harassment
A person who uses a computer or computer system, or who knowingly permits a device to be used, for any of the following purposes –
(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or
(b) threatening to inflict injury or physical harm to the person or property of any person, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding six months, or to both.

17. Cyber stalking
A person who wilfully, maliciously or repeatedly uses electronic communication to harass another person, or makes a threat with the intent to place that person in reasonable for his or her safety or for the safety of his or her immediate family, commits an offence and is liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

18. Offensive electronic communication
A person who maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

20. Revenge Pornography
A person who, by means of a computer or computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, commits an offence and is liable to a fine not exceeding P40,000, or to imprisonment for a term not exceeding two years, or to both.
23. Unlawful disclosure by service provider

A service provider who, without lawful authority, discloses –
(a) that an order under this Act has been made;
(b) any act done under an order; or
(c) any data collected or recorded under an order, commits an offence and is liable to a minimum fine of ₱1,000,000 but not exceeding ₱5,000,000.

24. Preservation order

A police officer or any person authorised by the Commissioner or by the Director, in writing, may, upon confirmation by the court and as soon as reasonably practical to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

25. Disclosure of preserved data

A police officer or any person authorised by the Commissioner or by the Director, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to-
(a) ensure that the data specified in the notice is preserved for the period specified in the notice; or
(b) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted.

26. Production Order

(1) A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, apply to a judicial officer for an order compelling –
(a) a person to submit specified data in that person’s possession or control, which is store in a computer system; and
(b) a service provider to submit subscriber information in relation to its services in that service provider’s possession or control.

(2) Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

28. Real time collection of content or traffic data

A police officer or any person authorized by the Commission or by the Director-General, in writing, may apply to a judicial office, ex-parte, for an order –
(a) for the collection or recording of content or traffic data, in real time, associated with specified communications transmitted by means of a computer or computer system; or
(b) compelling a service provider, within its technical capabilities, to –
(i) effect such collecting and recording referred to in paragraph (a), or
(ii) assist the person making the application to effect such collecting and recording.

32. Non-compliance with order or notice

A person who fails to comply with an order or notice issued under this Part commits an offence and is liable to a fine not exceeding ₱20,000 or to imprisonment for a term not exceeding one year, or to both.
A. Legislation on online harassment and cyber crimes cont

NAMIBIA

1. Cybercrimes Bill 2019 (not yet in force)

67. Electronic Harassment

A person who intentionally posts or sends a data message, or who intentionally causes a data message to be displayed –
(a) with the intention that it causes serious emotional distress to another person;
(b) which makes credible threats of violence or other harm;
(c) which contains a statement that the accused knows to be false or with reckless disregard whether it is true or false, and with the intention to do serious harm to the reputation of another person;
(d) which makes explicit sexual suggestions knowing it to be offensive or annoying to the person to whom it is directed;
(e) contains any pictorial representation of sexual activity or nudity of a specific person –
   (i) if that person has provided that information to the perpetrator privately and the person who provided that information has a reasonable expectation that the information should not be shared with other persons or the public; or
   (ii) if the photographic material has been created without the permission of the person depicted therein or the material has been obtained without the permission of the person depicted therein; or
   (iii) if that pictorial representation has been created by the manipulation of an image or photograph that does not depict sexual activity or nudity,

commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

70. Production order

(1) If a judge or magistrate is satisfied on the basis of an application by a member of the Namibian Police that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judge or magistrate may order that a person who has access to a computer system produce from the system specified computer data or a printout or other intelligible output of that data or that such person copy that data to a storage medium.

(2) A member of the Namibian police may apply for an order under subsection (1) to a judge or magistrate in chambers without hearing any other person.

71. Preservation

(1) If a member of the police is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation might be lost, modified or destroyed, that member of the police may issue a written notice instructing a person in control of that computer data to ensure that the data described in the notice must be preserved for the period specified in the notice which period may not be longer than seven days.

(2) An order referred to in subsection (1) may be extended by a judge or magistrate for a period that does not exceed three months at a time.

72. Interception and use of forensic tool

(1) A member of the Namibian police may intercept communications, or utilise a forensic tool if such action is authorised by a warrant issued by a judge in chambers which warrant may be issued if the judge believes after considering information on oath that -
   (a) a less intrusive method of investigation will not provide the information required;
   (b) the investigation is sufficiently important and the offence is sufficiently serious to justify the method specified in the warrant;
   (c) the information sought is relevant for the investigation of an offence under this Act or any other law or the common law.

(2) A warrant issued in terms of subsection (2), must be issued without notice to the person whose communications are to be intercepted or on whose computer system a remote forensic tool is to be installed.
(3) A warrant issued in terms of subsection (2) must state the action authorised.

(4) A warrant issued in terms of subsection (2) is valid for the period for which it has been issued, which period may not be longer than three months, but such warrant may be renewed on application for one or more further periods of no longer than three months at a time.

(5) An application for the issue of a warrant in terms of subsection (2) must be accompanied by a statement on oath by the applicant in which sufficient facts must be set out for the judge to decide the matters necessary to determine.

(6) If the judge considers it necessary, he or she may put any further questions to the applicant, which questions must be answered under oath by the applicant.

(7) The affidavit accompanying the application for a warrant to install a forensic tool, must explain the operation of the tool in sufficient detail to enable the judge to adequately assess the effect and operation of the tool.

(8) A warrant authorising the interception of communications, must specify which communications may be intercepted thereunder, which may be all the communications of a specified person.

(9) If a warrant authorises the installation of a forensic tool, it must state what kind of tool it authorises as well as specify on which computer system it will be installed and what method will be used to install that tool.

(10) A warrant issued in terms of subsection (2) authorises the police officer to perform all the actions stated therein.

(11) If a warrant is issued to intercept communications, it must be dealt with in terms of section (70(8) [sic] of the Communications Act, 2009 (Act No. 8 of 2009).

(12) Any person who provides telecommunications services, hosting, storage services or any other similar service to any other person must render any assistance specified in a warrant issued under this section.

(13) If it is expedient, a member of the Namibian police may be assisted by a staff member of the Namibian Central Intelligence Service in the performance of any action authorised by a warrant issued under this section.

(14) The provisions of this section in so far as they provide for a limitation on the fundamental right to privacy contemplated in Article 13 of the Namibian Constitution, are enacted upon the authority conferred by the said Article.

73. Revealing particulars of investigation

Any person who has become aware of any order or warrant issued under this Act and who-
(a) reveals any particular of the order or warrant to the person against whom the investigation is conducted;
(b) performs any other act that would render the investigation less effective, commits an offence and is on conviction liable to a fine not exceeding N$20 000 or to imprisonment for a period not exceeding five year[s] or to both such fine and such imprisonment.

2. Electronic Transactions Bill 2019 (not yet in force)

54. Take down notice

(1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include
(a) the full names and address of the complainant;
(b) the signature of the complainant;
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the service provider in respect of the complaint;
(f) telephonic and electronic contact details, if any, of the complainant;
(g) a statement that the complainant is acting in good faith;
(h) a statement by the complainant that the information in the take down notice is to his or her knowledge true and correct.

(2) A service provider is not liable for wrongful take down in a bona fide response to a notification of unlawful activity which complies with subsection (1).

(3) If a service provider removes material in compliance with a take down notice, the service provider must notify the person by whom the information has been made available within three days from such take down.

(4) A person who has been notified of such take down may object to such take down by giving notice of such objection and the reason for such objection to the service provider concerned.
A. Legislation on online harassment and cyber crimes cont

(5) If an objection has been received by the service provider, it must be forwarded to the person who requested the take down of the information.

(6) The person who requested the take down may provide further information to the service provider within three days from the receipt of the objection.

(7) If after the receipt of the information referred to in subsection (6) or if the period for providing that information has passed, the service provider must restore the information if he or she has a bona fide belief that the information may reasonably be lawful.

(8) Any person who makes a false or misleading statement in-
(a) a request for a take down notice;
(b) a notice referred to in subsection (4); or
(c) further information provided in terms of subsection (6), commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

Author’s Note The following excerpt on the take-down provisions was made in the submissions on the draft Provisions of the Electronic Transactions and Cybercrime Bill 2017 by the Access to Information Namibia (ACTION) Coalition1, which would have the effect that removal of information cannot occur before notice and opportunity is given to the person who made the information available:

“3.6. We are also extremely concerned at the ‘take down’ obligations imposed upon service providers in response to a take down notice as provided for in section 54 of the Bill. In this regard:
3.6.1. These provisions are extremely broad and do not sufficiently protect the public interest in the free flow of information, particularly online
3.6.2. We are also concerned that service providers, who cannot be expected to have legal training, will be expected to assess whether or not a take down notice does or does not set out an adequate case in respect of alleged ‘unlawful activity’ as required;
3.6.3. Consequently, we are of the view that these can be easily manipulated and abused;
3.6.4. We are of the view that bona fide news media online services may be subject to take down notices which do not in fact reveal unlawful activity with potentially damaging effects on both the expression rights of the news media and the information rights of the public;
3.6.5. We are of the view that protections need to be built to preserve the information rights of the public and to make the default position be that publications are accessible and not immediately censored by a service provider in response to a takedown notice on pain of being liable for a wrongful take down. Happily this can be effected by a few wording changes to the provisions of section 54 of the Bill.

3.7. Consequently we suggest the following amendments to section 54 of the Bill:
3.7.1. that the word ‘not’ be removed from subsection 54(2);
3.7.2. that the word ‘removes’ is deleted from subsection 54(3) and is substituted with the words ‘is requested to remove’; and
3.7.3. that the word ‘restore’ is deleted from subsection 54(7) and is substituted with the word ‘remove’; and
3.7.4. the word ‘lawful’ be is deleted from subsection 54(7) and is substituted with the word ‘unlawful’.”

55. No general obligation to monitor

When providing the services contemplated in this Chapter there is no general obligation on a service provider to -
(a) monitor the data which it transmits or stores; and
(b) actively seek facts or circumstances indicating an unlawful activity.

56. Regulations relating to take down notices

The Minister may make regulations
(a) prescribing the form of or any procedural requirement of notices under this Chapter;
(b) the manner and content of information to be provided by service providers in order to assist members of the public to comply with the provisions of this Chapter.

1  ACTION Access To Information Namibia, Submissions on the Draft Provisions of the Electronic Transactions and Cybercrime Bill 2017, 13 September 2017, pp.4 - 5:
**SOUTH AFRICA**

1. Protection from Harassment Act 2011

1. Definitions and application of the Act

“electronic communications service provider” means an entity or a person who is licensed or exempted from being licensed in terms of Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005) to provide an electronic communications service.

4. Electronic communications service provider to furnish particulars to court

(1) If an application for a protection order is made in terms of section 2 and the court is satisfied in terms of section 3(2) that a protection order must be issued as a result of the harassment of the complainant or a related person by means of electronic communications or electronic mail over an electronic communications system of an electronic communications service provider and the identity or address of the respondent is not known, the court may—
(a) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and
(b) issue a direction in the prescribed form directing an electronic communications service provider to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—
(i) the electronic communications identity number from where the harassing electronic communications or electronic mail originated;
(ii) the name, surname, identity number and address of the respondent to whom the electronic communications identity number has been assigned;
(iii) any information which indicates that electronic communications or electronic mail were or were not sent from the electronic communications identity number of the respondent to the electronic communications identity number of the complainant; and
(iv) any other information that is available to an electronic communications service provider which may be of assistance to the court to identify the respondent or the electronic communications service provider which provides a service to the respondent.

(2) If the court issues a direction in terms of subsection (1) the court must direct that the direction be served on the electronic communications service provider in the prescribed manner.

(3) (a) The information referred to in subsection (1)(b)(i), (ii) and (iii) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.
(b) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for—
(i) an extension of the period of five ordinary court days referred to in paragraph (a) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or
(ii) the cancellation of the direction on the grounds that—
(aa) it does not provide an electronic communications service to either the respondent or complainant or related person; or
(bb) the requested information is not available in the records of the electronic communications service provider.

(4) After receipt of an application in terms of subsection (3)(b), the court—
(a) must consider the application;
(b) may, in the prescribed manner, request such additional evidence by way of affidavit from the electronic communications service provider as it deems fit;
(c) must give a decision in respect thereof; and
(d) must inform the electronic communications service provider in the prescribed form and in the prescribed manner of the outcome of the application.

(5) (a) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1)(b)(i) and (ii), consider the issuing of an interim protection order in terms of section 3(2) against the respondent on the date to which the proceedings have been adjourned.
A. Legislation on online harassment and cyber crimes cont

(b) Any information furnished to the court in terms of subsection (1)(b)(iii) forms part of the evidence that a court may consider in terms of section 3(1).

(6) An electronic communications service provider must, at least 48 hours before providing the information referred to in subsection (1)(b) to the court, by means of an electronic communication, inform the respondent of the-
(a) information that is to be provided to the court;
(b) reference number of the direction; and
(c) name and address of the court.

(7) (a) The Director-General: Justice and Constitutional Development must, in consultation with the Director-General: Communications and the electronic communications service providers, compile and maintain a list of electronic communications service providers that can provide the courts with the information referred to in subsection (1)(b) and must contain the following particulars of each such electronic communications service provider:
(i) the name and address (physical and postal address);
(ii) the e-mail address;
(iii) a telephone and facsimile number; and
(iv) the names of persons who are responsible for providing the information referred to in subsection (1)(b).

(b) An electronic communications service provider must, in the prescribed manner and without undue delay, bring any change of any of the particulars referred to in paragraph (a) to the attention of the Director-General: Justice and Constitutional Development.

(c) The Director-General: Justice and Constitutional Development must, in the prescribed manner and without undue delay, make the list referred to in paragraph (a) and any subsequent amendments thereto available to all courts.

(8) The Minister may, after consultation with the electronic communications service providers, by notice in the Gazette, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection 1(b).

5. Court may order investigation to ascertain name and address of respondent

(1) If an application for a protection order is made in terms of section 2 and the court is satisfied in terms of section 3(2) that a protection order must be issued as a result of the harassment of the complainant or a related person and the identity or address of the respondent is not known, the court may-
(a) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and
(b) issue a direction in the prescribed form directing the station commander of the relevant police station to investigate the matter with a view to determining the name and address of the respondent or obtaining any other information which may be required in order to identify or trace the respondent.

(2) If the court issues a direction in terms of subsection (1) the court must direct that the direction be served on the station commander of the relevant police station in the prescribed manner by the clerk of the court or sheriff identified by the court.

(3) (a) The information referred to in subsection (1)(b) must be provided to the court by means of an affidavit in the prescribed form within the time period indicated by the court.

(b) A station commander on which a direction is served, may, in the prescribed manner by means of an affidavit in the prescribed form, apply to the court for-
(i) an extension of the period referred to in paragraph (a) on the grounds that the information cannot be provided timeously; or
(ii) the cancellation of the direction on the grounds that, after a reasonable investigation of the matter, the South African Police Service is not in a position to determine the name and address of the respondent or obtain any other information which is required in order to identify or trace the respondent.

(4) After receipt of an application in terms of subsection (3)(b), the court-
(a) must consider the application;
(b) may, in the prescribed manner, request such additional evidence by way of affidavit from the station commander as it deems fit;
(c) must give a decision in respect thereof; and
(d) must inform the station commander, in the prescribed form and in the prescribed manner, of the outcome of the application.

(5) The court may, on receipt of an affidavit in terms of subsection (3)(a) which contains the information provided for in subsection (1)(b), consider the issuing of an interim protection order in terms of section 3(2) against the respondent on the date to which the proceedings have been adjourned.

18. Offences

(1) Notwithstanding the provisions of any other law, any person who-

(a) contravenes any prohibition, condition, obligation or order imposed in terms of section 10(1) or (2);

(b) in an affidavit referred to in section 11(4)(a), makes a false statement in a material respect, is guilty of an offence and liable on conviction to a fine or imprisonment for a period not exceeding five years.

(2) Any person who reveals the identity or address of any person in contravention of section 8(1)(b) or who publishes any information in contravention of section 8(1)(c), is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

(3) Any person who contravenes or fails to comply with section 7(3) is guilty of an offence and is liable on conviction to a fine or to imprisonment not exceeding three months.

(4) (a) Any electronic communications service provider or employee of an electronic communications service provider who—

(i) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of section 4(3)(a) or such extended period allowed by the court in terms of section 4(3)(b);

(ii) makes a false statement in an affidavit referred to in section 4(1)(b), (3)(b) or (4)(b) in a material respect; or

(iii) fails to comply with section 4(6), is guilty of an offence.

(b) Any electronic communications service provider or employee of an electronic communications service provider who is convicted of an offence referred to in paragraph (a), is liable, in the case of—

(i) an electronic communications service provider, to a fine not exceeding R10,000; or

(ii) an employee of an electronic communications service provider to a fine or to imprisonment for a period not exceeding six months.

(5) Any person who in terms of section 6(2) is requested to furnish his or her name and address or any other information to a member of the South African Police Service and who fails to do so or who furnishes a false or incorrect name and address or other information, is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding six months.

2. Cybercrimes Bill 2017 (not yet in force)

...
A. Legislation on online harassment and cyber crimes cont

15. Data message which threatens persons with damage to property or violence

(1) A person commits an offence if he or she unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which -

(a) threatens a person with-

(i) damage to property belonging to, or violence against, that person; or

(ii) damage to property belonging to, or violence against a related person; or

(b) threatens-

(i) a group of persons;

(ii) any person forming part of that group of persons; or

(iii) any person associated with that group of persons, with damage to property belonging to, or violence against-

(aa) that group of persons;

(bb) any person who forms part of that group of persons; or

(cc) any person who is associated with that group of persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message, either by itself or in conjunction with any other data message, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph (a) or (b), respectively.

16. Distribution of data message of intimate image

(1) Any person (“A”) who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of a person (“B”) without the consent of B, is guilty of an offence.

(2) For purposes of subsection (1)-

(a) “B” means-

(i) the person who can be identified as being displayed in the data message;

(ii) any person who is described as being displayed in the data message, irrespective of the fact that he or she cannot be identified as being displayed in the data message; or

(iii) any person who can be identified from other information as being displayed in the data message; and

(b) “intimate image” means a depiction of a person-

(i) real or simulated and made by any means in which-

(aa) B is nude, or his or her genital organs or anal region, or if B is a female, her breasts, are displayed; or

(bb) the covered genital or anal region of B, or if B is a female, her covered breasts, are displayed in a manner that violates or offends the sexual integrity or dignity of B; and

(ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made.

17. Data message which is harmful [This provision is no longer included in the 2017 draft.]

(1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

(2) For purposes of subsection (1), a data message is harmful when-

(a) it threatens a person with-

(i) damage to any property belonging to, or violence against, that person; or

(ii) damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;

(b) it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

(c) it intimidates, encourages or harasses a person to harm himself or herself or any other person; or

(d) it is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.

19. Sentencing

(7) Any person who contravenes the provisions of section 14, 15 or 16 is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.
54. Obligations of electronic communications service providers and financial institutions

(1) An electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must—
   (a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and
   (b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

(2) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must by notice in the Gazette, prescribe -
   (a) the category or class of offences which must be reported to the South African Police Service in terms of subsection (1); and
   (b) the form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service.

(3) An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000.

(4) Subject to any other law, or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic service provider or financial institution to—
   (a) monitor the data which the electronic communications service provider or financial institution transmits or stores; or
   (b) actively seek facts or circumstances indicating any unlawful activity.

(5) This Chapter does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

TANZANIA

The Cybercrimes Act 2015

16. Publication of False Information

Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with the intent to defame, threaten, abuse, insult or otherwise deceive or mislead the public or counselling [sic] the commission of an offence commits an offence, and shall on conviction be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three year[s] or to both.

...  

20. Unsolicited messages

(1) A person shall not, with intent to commit an offence under this Act—
    (a) initiate the transmission of unsolicited messages;
    (b) relay or transmit unsolicited messages, or
    (c) falsify header information in unsolicited messages.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or three times the value of undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or to both.

(3) For the purpose of this section, “unsolicited messages” means any electronic message which is not solicited by the recipient.

...  

22. Obstruction of investigation

(1) A person who intentionally and unlawfully destroy, delete, alter, conceal, modify, renders computer data meaningless, ineffective or useless with intent to obstruct or delay investigation commits an offence and on conviction, is liable to a fine of not less than three million shillings or to imprisonment for a term not less than one year or both.
A. Legislation on online harassment and cyber crimes

(2) A person who intentionally and unlawfully prevents the execution or fails to comply with an order issued under this Act, commits an offence and is liable, on conviction, to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both.

23. Cyber bullying

(1) A person shall not initiate or send any electronic communication using a computer system to another person with the intent to coerce, intimidate, harass or cause emotional distress.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both.

UGANDA

Computer Misuse Act 2011

9. Preservation Order

(1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—
   (a) until such time as may reasonably be required for the investigation of an offence; or
   (b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.

10. Disclosure of Preservation Order

The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—
   (a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or
   (b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.

11. Production Order

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling—
   (a) any person to submit specified data in that person’s possession or control, which is stored in a computer system; and
   (b) any service provider offering its services to submit subscriber information in relation to such services in that service provider’s possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

PART III—COMPUTER MISUSE OFFENCES.

24. Cyber harassment

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

(2) For purposes of this section cyber harassment is the use of a computer for any of the following purposes—
   (a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;
   (b) threatening to inflict injury or physical harm to the person or property of any person; or
   (c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.
25. Offensive communication

Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both.

26. Cyber stalking

Any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person’s immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

27. Compensation

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

ZIMBABWE

Cybercrime and Cybersecurity Bill 2017 (draft - not yet in force)

15. Sending threatening data message

Any person who unlawfully and intentionally by means of a computer or information system sends any data message to another person threatening harm to the person or the person’s family or friends or damage to the property of such persons shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

16. Cyber-bullying and harassment

Any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

17. Transmission of false data message intending to cause harm

Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

19. Transmission of intimate images without consent

(1) Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes a data message containing any intimate image of an identifiable person without the consent of the person concerned causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) For the purposes of subsection (1) “intimate image” means a visual depiction of a person made by any means in which the person is nude, the genitalia or naked female breasts are exposed or sexual acts are displayed.
A. Legislation on online harassment and cyber crimes cont

Commonwealth Asia

SINGAPORE

Protection from Harassment 2014 (as amended by the Protection from Harassment (Amendment) Act 2019)

2. Interpretation

“communication” means any words, image (moving or otherwise), message, expression, symbol or other representation that can be seen, heard or otherwise perceived by any person, or any combination of these;

“identity information” means any information that, on its own or with other information, identifies or purports to identify an individual, including (but not limited to) any of the following:
(a) the individual’s name, residential address, postal address, email address, telephone number, date of birth, national identity number, passport number, signature (whether handwritten or electronic) or password;
(b) any photograph or video recording of the individual;
(c) any information about the individual’s family, employment or education.

“internet intermediary” means a person who provides any internet intermediary service;

“internet intermediary service” means -
(a) a service that allows end-users to access materials originating from third parties, using the internet;
(b) a service of transmitting materials to end-users on or through the internet; or
(c) a service of displaying, to an end-user who uses the service to make an online search, an index of search results, each of which links that end-user to content hosted or stored at a location which is separate from the location of the index of search results,

but excludes any act done for the purpose of or that is incidental to the provision of -
(d) a service of giving the public access to the internet; or
(e) a computing resource service;

Examples of internet intermediary services are —
(a) social networking services;
(b) search engine services;
(c) content aggregation services;
(d) internet-based messaging services; and
(e) video-sharing services;

PART 2 - OFFENCES

3. Intentionally causing harassment, alarm or distress

(1) An individual or entity must not, with intent to cause harassment, alarm or distress to another person (called in this section the target person), by any means -
(a) use any threatening, abusive or insulting words or behaviour;
(b) make any threatening, abusive or insulting communication; or
(c) publish any identity information of the target person or a related person of the target person, and as a result causing the target person or any other person (each called in this section the victim) harassment, alarm or distress.

(2) Any individual or entity that contravenes subsection (1) shall be guilty of an offence and, imprisonment for a term not exceeding 6 months or to both.

(3) In any proceedings for an offence under subsection (2), it is a defence for the accused individual or accused entity (called in this section the accused) to prove that the accused’s conduct was reasonable.
Illustrations

These acts are acts associated with stalking of X by Y:

(a) X and Y are co-workers. At the workplace, X loudly and graphically describes to the other co-workers X’s desire for a sexual relationship with Y in an insulting manner. X knows that Y is within earshot and intends to cause Y distress. Y is distressed. X is guilty of an offence under this section.

(b) X writes a letter containing threatening words towards Y intending to send the letter to Y to cause him alarm. X decides not to send the letter and throws it away. Y finds the letter and is alarmed. X is not guilty of an offence under this section as he had no reason to believe that the letter would be seen by Y.

(c) X and Y were formerly in a relationship which has since ended. X writes a post on a social media platform making abusive and insulting remarks about Y’s alleged sexual promiscuity. In a subsequent post, X includes Y’s photographs and personal mobile number, intending to cause Y harassment by facilitating the identification or contacting of Y by others. Y did not see the posts, but receives and is harassed by telephone calls and SMS messages from strangers (who have read the posts) propositioning Y for sex. X is guilty of an offence under section 3(2) in relation to each post.

(d) X records a video of Y driving recklessly in a car on the road. X posts the video on an online forum, where people share snippets of dangerous acts of driving on the road. X posts the video with the intent to warn people to drive defensively. X has not committed an offence under this section...

Division 2 — Orders relating to false statements

15. General provisions applicable to orders under sections 15A to 15E

(1) This section applies to the following orders:
   (a) a stop publication order;
   (b) a correction order;

(2) An order mentioned in subsection (1) takes effect in respect of a relevant party -
   (a) when the order is served on the relevant party in such manner as may be prescribed;
   (b) where a court dispenses with the service of the order, when the service of the order on the relevant party is dispensed with by a court; or
   (c) at such later time as a court may specify.

(3) An order mentioned in subsection (1) may be made in respect of a false statement of fact even if the false statement has been amended or has ceased to be published.

(4) An order mentioned in subsection (1) may -
   (a) be made against a relevant party whether or not the relevant party is in or outside Singapore, is incorporated or established in or outside Singapore, or has its management or control in or outside Singapore; and
   (b) require a relevant party to do or refrain from doing an act in or outside Singapore.

(5) A court may vary, suspend or cancel an order mentioned in subsection (1), on the application of-
   (a) the subject or the author of the false statement;
   (b) the relevant party; or
   (c) an individual or entity that published the relevant statement to which the order relates.

(6) An order mentioned in subsection (1) ceases to have effect -
   (a) during any period when the order is suspended under subsection (5); and
   (b) when the order expires, or is cancelled under subsection (5).

15A. Stop publication order

(1) A court may, on an application by the subject of an alleged false statement of fact (called in this section the relevant statement), make a stop publication order against any individual or entity (called in this section the respondent), if -
   (a) the court is satisfied on the balance of probabilities that -
      (i) the respondent has published the relevant statement; and
      (ii) the relevant statement is a false statement of fact; and
   (b) it is just and equitable in the circumstances to make the stop publication order.

(2) A stop publication order may be made against a respondent even if the respondent does not know or have reason to believe that the relevant statement is false.

(3) A stop publication order may require the respondent or any other individual or entity to stop publishing the relevant statement, and not to publish any substantially similar statement, by a specified time.
A. Legislation on online harassment and cyber crimes cont

(4) In this section —
   (a) “specified” means specified in the stop publication order; and
   (b) the respondent or any other individual or entity does not publish a statement merely by doing any act for the purpose of, or that is incidental to, the provision of -
      (i) an internet intermediary service;
      (ii) a telecommunication service;
      (iii) a service of giving the public access to the internet; or
      (iv) a computing resource service.

15B. Correction order

(1) A court may, on an application by the subject of an alleged false statement of fact (called in this section a relevant statement), make a correction order against an individual or entity (called in this section the respondent), if -
   (a) the court is satisfied on the balance of probabilities that -
      (i) the respondent has published the relevant statement; and
      (ii) the relevant statement is a false statement of fact; and
   (b) it is just and equitable in the circumstances to make the correction order.

(2) A correction order may be made against a respondent even if the respondent does not know or have reason to believe that the relevant statement is false.

(3) A correction order may require the respondent to publish in Singapore a correction notice, within a specified time -
   (a) to any specified person or description of persons; and
   (b) in a specified form and manner, which may include publication -
      (i) at a specified online location or in a specified newspaper or other printed publication of Singapore; or
      (ii) in specified proximity to every copy of the relevant statement, or of any substantially similar statement, that is published by the respondent.

(4) A correction notice must contain all or any of the following as may be specified in the correction order:
   (a) a statement, in such terms as may be specified, that the court has determined the relevant statement is false, or that such material as may be specified contains a false statement of fact;
   (b) a statement, in such terms as may be specified, correcting the false statement of fact, or a reference to a specified location where such a statement may be found.

(5) In this section -
   (a) “specified” means specified in the correction order; and
   (b) the respondent does not publish a statement merely by doing any act for the purpose of, or that is incidental to, the provision of -
      (i) an internet intermediary service;
      (ii) a telecommunication service;
      (iii) a service of giving the public access to the internet; or
      (iv) a computing resource service.

15C. Disabling order

(1) A court may, on an application by the subject of an alleged false statement of fact (called in this section the relevant statement), make a disabling order against an internet intermediary (called in this section the respondent) if -
   (a) the court is satisfied on the balance of probabilities that -
      (i) any material consisting of or containing the relevant statement has been or is being published by means of an internet intermediary service provided by the respondent; and
      (ii) the relevant statement is a false statement of fact; and
   (b) it is just and equitable in the circumstances to make the disabling order.

(2) A disabling order may require the respondent to disable access by end-users of the internet intermediary service provided by the respondent in Singapore, within a specified time, to -
   (a) any specified material provided on or through the service that consists of or contains the relevant statement; and
   (b) where the respondent is a prescribed internet intermediary — the specified material mentioned in paragraph (a) or any identical copies of the specified material.

(3) An end-user who accesses a part of any material is taken to access the material.
15D. Targeted correction order

(1) A court may, on an application by the subject of an alleged false statement of fact (called in this section the relevant statement), make a targeted correction order against an internet intermediary (called in this section the respondent) if -
   (a) the court is satisfied on the balance of probabilities that -
      (i) any material consisting of or containing the relevant statement has been or is being published by means of an internet intermediary service provided by the respondent; and
      (ii) the relevant statement is a false statement of fact; and
   (b) it is just and equitable in the circumstances to make the targeted correction order.

(2) A targeted correction order may require the respondent to publish a targeted correction notice -
   (a) by means of the internet intermediary service, to all end-users in Singapore who access any specified material provided on or through the service that consists of or contains the relevant statement from any specified time; and
   (b) where the respondent is a prescribed internet intermediary — by any means and by a specified time, to all end-users in Singapore that the respondent knows had accessed the specified material mentioned in paragraph (a) or any identical copies of the specified material by means of the internet intermediary service.

(3) A targeted correction notice must contain all or any of the following as may be specified in the targeted correction order:
   (a) a statement, in such terms as may be specified, that the court has determined the specified material consists of or contains a false statement of fact;
   (b) a statement, in such terms as may be specified, correcting the false statement of fact, or a reference to a specified location where the statement may be found.

(4) An end-user who accesses a part of any material is taken to access the material.

15E. General correction order

(1) A court may, on an application by the subject of an alleged false statement of fact (called in this section the relevant statement), make a general correction order against a prescribed individual or entity (called in this section the respondent), if -
   (a) the court is satisfied on the balance of probabilities that -
      (i) the relevant statement is a false statement of fact; and
      (ii) the publication of the relevant statement has caused or is likely to cause serious harm to the reputation of the subject; and
   (b) it is just and equitable in the circumstances to make the general correction order.

(2) A general correction order may require the respondent to publish in Singapore a general correction notice within a specified time in a specified form and manner -
   (a) where the respondent is a prescribed holder of a permit under section 21 of the Newspaper and Printing Presses Act (Cap. 206) — in a specified newspaper or other printed publication, printed or published by the respondent;
   (b) where the respondent is a prescribed broadcasting licensee within the meaning of the Broadcasting Act (Cap. 28) — by a specified broadcasting service provided by the respondent;
   (c) where the respondent is a prescribed holder of a licence under section 5 of the Telecommunications Act (Cap. 323) — by a specified telecommunication system or service run by the respondent;
   (d) where the respondent is a prescribed internet intermediary -
      (i) by a specified internet intermediary service provided by the respondent; or
      (ii) to all end-users, or a specified class of end-users, in Singapore who use that internet intermediary service at any time after the general correction order is served; and
   (e) in any other case—by any specified means within the control of the respondent.

(3) A general correction notice must contain all or any of the following as may be specified in the general correction order:
   (a) a statement, in such terms as may be specified, that the court has determined that the relevant statement is false;
   (b) a statement, in such terms as may be specified, correcting the false statement of fact, or a reference to a specified location where the statement may be found.

(4) In this section, “specified” means specified in the general correction order.

Illustrations

(a) X publishes a false statement that Y, a lawyer, had misappropriated client moneys. As a result, Y’s clients terminate their contracts for Y’s services. Y has suffered serious harm to Y’s reputation.

(b) X makes a false statement that Y, a married female, had committed adultery with multiple men. The statement is widely published on social media. Y has suffered serious harm to Y’s reputation.
A. Legislation on online harassment and cyber crimes cont

16. General provisions applicable to interim orders

(1) Where an application by the subject of an alleged false statement of fact (called in this section and sections 16A and 16B a relevant statement) for an order mentioned in paragraph (a) or (b) is pending against a respondent in relation to that application, the subject may also apply for the interim order mentioned in that paragraph to be made against that respondent:
   (a) a stop publication order—an interim stop publication order or an interim notification order;
   (b) a correction order — an interim notification order.

(2) Sections 16A and 16B apply despite any of the following:
   (a) that notice of the application has not been served on the respondent;
   (b) that notice of the application has not been served, within a reasonable time before the hearing of the application, on the respondent.

(3) An interim order takes effect in respect of the respondent-
   (a) when the order is served on the respondent in such manner as may be prescribed;
   (b) where the court dispenses with the service of the order, when the service of the order on the respondent is dispensed with by the court; or
   (c) at such later time as the court may specify.

(4) An interim order under this section may be made in respect of a relevant statement even if the statement has been amended or has ceased to be published in Singapore.

(5) There is no appeal against a decision of the court in relation to an interim order under this section.

(6) The court may vary, suspend or cancel an interim order under this section, on the application of—
   (a) the subject or author of the relevant statement;
   (b) the respondent; or
   (c) an individual or entity that published the relevant statement.

(7) An interim order made under this section remains in effect until it expires, or is cancelled under subsection (6).

(8) An interim order under this section may be made subject to such exceptions or conditions as may be specified in the order.

16A. Interim stop publication order

(1) A court may make an interim stop publication order against the respondent in relation to an application for a stop publication order if—
   (a) the court is satisfied that there is prima facie evidence that—
      (i) the respondent published or continues to publish the relevant statement;
      (ii) the relevant statement is a false statement of fact; and
      (iii) the publication of the relevant statement by the respondent has caused or is likely to cause the subject harm; and
   (b) it is just and equitable in the circumstances to make the stop publication order on an expedited basis.

(2) Section 15A(2), (3) and (4) applies to an interim stop publication order as it applies to a stop publication order.

16AA. Interim disabling order

(1) A court may make an interim disabling order against the respondent in relation to an application for a disabling order if—
   (a) the court is satisfied that there is prima facie evidence that—
      (i) any material consisting of or containing the relevant statement (called in this section the specified material) has been or is being published by means of an internet intermediary service provided by the respondent;
      (ii) the relevant statement is a false statement of fact; and
      (iii) the publication of the specified material by means of the service has caused or is likely to cause the subject harm; and
   (b) it is just and equitable in the circumstances to make the disabling order on an expedited basis.

(2) Section 15C(2) and (3) applies to an interim disabling order as it applies to a disabling order.
16B. Interim notification order

(1) A court may make an interim notification order against the respondent in relation to an application for a correction order or a stop publication order if -
   (a) the court is satisfied that there is prima facie evidence that -
       (i) the respondent published or continues to publish the relevant statement;
       (ii) the relevant statement is a false statement of fact; and
       (iii) the publication of the relevant statement by the respondent has caused or is likely to cause the subject harm; and
   (b) it is just and equitable in the circumstances to make the interim notification order.

(2) An interim notification order may require the respondent to publish an interim notice, within a specified time -
   (a) to any specified person or description of persons; and
   (b) in a specified form and manner, which may include publication -
       (i) at a specified online location or in a specified newspaper or other printed publication of Singapore; or
       (ii) in specified proximity to every copy of the relevant statement, or of any substantially similar statement,
       that is published by the respondent.

(3) An interim notice must -
   (a) state that there is a pending application for a correction order or a stop publication order or both (as the case may be) in respect of the relevant statement; and
   (b) be in such form and published in such manner as may be specified in the interim notification order.

(4) Section 15B(2) and (5) applies to an interim notification order as it applies to a correction order.

16BA. Targeted interim notification order

(1) A court may make a targeted interim notification order against the respondent in relation to an application for a targeted correction order if -
   (a) the court is satisfied that there is prima facie evidence that -
       (i) the relevant statement is being published by means of an internet intermediary service provided by the respondent;
       (ii) the relevant statement is a false statement of fact; and
       (iii) the publication of the specified material by means of the service has caused or is likely to cause the subject harm; and
   (b) it is just and equitable in the circumstances to make the targeted interim notification order.

(2) A targeted interim notification order may require the respondent to publish a targeted interim notice -
   (a) by means of the internet intermediary service to all end-users in Singapore who access any specified material provided on or through the service that consists of or contains the false statement from any specified time; and
   (b) where the respondent is a prescribed internet intermediary — by any means and by a specified time, to all end-users in Singapore that the respondent knows had accessed the specified material mentioned in paragraph (a) or any identical copies of the specified material by means of the internet intermediary service.

(3) A targeted interim notice must -
   (a) state that there is a pending application for a targeted correction order in respect of the specified material; and
   (b) be in such form and published in such manner as may be specified in the targeted interim notification order.

(4) An end-user who accesses a part of any material is taken to access the material.

16BB. Publication of notices

(1) A person who is required to publish any of the following notices must ensure that they are easily perceived:
   (a) a targeted correction notice;
   (b) a general correction notice;
   (c) a targeted interim notice.

(2) Subject to subsection (3), a notice is easily perceived if -
   (a) a notice (not being an audio recording) is conspicuous, regardless of the type of platform or device used by the end-user or viewer;
A. Legislation on online harassment and cyber crimes cont

Illustration
A notice that is in a text form is conspicuous if it is sufficiently differentiated from the background and is of a reasonable type size compared to the rest of the text on the same page.
(b) the notice is easy to read, view or listen to, and not easy to miss;

Illustrations
(a) Where the notice is an audio recording, it is easy to listen to it if it is in a volume and cadence sufficient for it to be heard and understood.
(b) Where the notice is a video recording or a dynamic display, it is easy to view if it appears for a duration sufficient for it to be viewed and understood.
(c) A notice that is in a text form or the form of a video recording or dynamic display is easy to miss if it is contained in a pop-up window, insofar as access to it may be easily disabled.
(c) the notice (not being an audio recording) is placed near the subject statement (where relevant), and in a location where end-users or viewers are likely to look; or
(d) the end-user is required to access another online location in order to comprehend the notice.

Illustration
An example of such requirement is the mere provision of a hyperlink to the notice or a part of it.
(3) For the purposes of this section, without limiting the manner of complying with subsection (1), a notice is taken to be easily perceived if the notice is published in accordance with such measures as may be prescribed by regulations made under section 20 (called in this section the prescribed measures).
(4) The measures required to be taken under a targeted correction order, general correction order or targeted interim notification order must not be inconsistent with the prescribed measures.

Author’s Note  In May 2019, Singapore passed a Criminal Law Reform Act 2019 that includes provisions on distributing or threatening to distribute an intimate image or recording, and voyeurism (ss.377BB-377BE). These are not quoted here as they do not incorporate any elements not included in the other examples cited.
Commonwealth Caribbean and Americas

CANADA
NOVA SCOTIA

Intimate Images and Cyber-protection Act 2017

3. Interpretation

(c) “cyber-bullying” means an electronic communication, direct or indirect, that causes or is likely to cause harm to another individual’s health or well-being where the person responsible for the communication maliciously intended to cause harm to another individual’s health or well-being or was reckless with regard to the risk of harm to another individual’s health or well-being, and may include

(i) creating a web page, blog or profile in which the creator assumes the identity of another person,
(ii) impersonating another person as the author of content or a message,
(iii) disclosure of sensitive personal facts or breach of confidence,
(iv) threats, intimidation or menacing conduct,
(v) communications that are grossly offensive, indecent, or obscene,
(vi) communications that are harassment,
(vii) making a false allegation,
(viii) communications that incite or encourage another person to commit suicide,
(ix) communications that denigrate another person because of any prohibited ground of discrimination listed in Section 5 of the Human Rights Act, or
(x) communications that incite or encourage another person to do any of the foregoing.

(e) “electronic communication” means any form of electronic communication, including any text message, writing, photograph, picture recording or other matter that is communicated electronically;

(f) “intimate image” means a visual recording of a person made by any means, including a photograph, film or video recording,

(i) in which a person depicted in the image is nude, is exposing the person’s genital organs, anal region or her breasts, or is engaged in explicit sexual activity,
(ii) that was recorded in circumstances that gave rise to a reasonable expectation of privacy in respect of the image, and
(iii) where the image has been distributed, in which the person depicted in the image retained a reasonable expectation of privacy at the time it was distributed;

4. Expectation of privacy not lost

(1) A person depicted in an intimate image does not lose the person’s expectation of privacy in respect of the image if the person consented to another person recording the image in circumstances where the other person knew or ought reasonably to have known that the image was not to be distributed to any other person.

(2) A person depicted in an intimate image does not lose the person’s expectation of privacy in respect of the image if the person provided the image to another person in circumstances where the other person knew or ought reasonably to have known that the image was not to be distributed to any other person.

5. Application to Court

(1) An individual whose intimate image was distributed without consent or who is or was the victim of cyber-bullying may apply to the Court for an order under Section 6.

(2) Where the individual referred to in subsection (1) is a minor, that individual’s parent or guardian may apply to the Court for an order under Section 6.

(3) Subject to subsection (4) and the regulations, the applicant shall name as a respondent

(a) the person alleged to have distributed an intimate image without consent or to have cyber-bullied;
A. Legislation on online harassment and cyber crimes cont

(b) where the application identifies an electronic device, Internet Protocol address, website, electronic user name or account, electronic mail address or other unique identifier as being or having been used for the distribution of intimate images without consent or cyber-bullying,
   (i) the owner of the electronic device,
   (ii) any person who has been assigned or has control over the use of the Internet Protocol address, or
   (iii) the user or person responsible for the website, user name or account, electronic mail address or other unique identifier;
(c) where the person referred to in clause (a) or (b) is a minor, the parent or guardian of the person;
(d) any other person against whom an order is sought; and
(e) any other person as directed by the Court.

(4) An application under this Section must identify the respondent by name or, where the name of the respondent is not known, by the Internet Protocol address, website, username or account, electronic mail address or other unique identifier used for intimate image distribution or cyber-bullying.

6. Order

(1) Where the Court is satisfied that a person has engaged in cyber-bullying or has distributed an intimate image without consent, the Court may make one or more of the following orders:
   (a) an order prohibiting the person from distributing the intimate image;
   (b) an order prohibiting the person from making communications that would be cyber-bullying;
   (c) an order prohibiting the person from future contact with the applicant or another person;
   (d) an order requiring the person to take down or disable access to an intimate image or communication;
   (e) an order declaring that an image is an intimate image;
   (f) an order declaring that a communication is cyber-bullying;
   (g) an order referring the matter to dispute-resolution services provided by the agency or otherwise;
   (h) an order provided for by the regulations;
   (i) any other order which is just and reasonable.

(2) Where it is shown that the distribution of an intimate image without consent or cyber-bullying has occurred, the Court may order any person to do one or more of the following:
   (a) provide to the applicant any information in the possession of the person that may help identify a person who may have used an Internet Protocol address, website, electronic username or account, electronic mail address or other unique identifier that may have been used to distribute an intimate image without consent or for cyber-bullying;
   (b) take down or disable access to an intimate image or cyber-bullying communication;
   (c) perform such other action as the Court considers just and reasonable.

(3) Where the Court is satisfied that a person has distributed an intimate image without consent or has engaged in cyber-bullying, the Court may
   (a) order the person to pay general, special, aggravated or punitive damages to the person depicted in the intimate image or the victim of cyber-bullying; and
   (b) order the person to account for profits.

(4) In awarding damages under clause (3)(a), the Court shall not have regard to any order made under clause (3)(b).

(5) An order made under this Section may be interim or final and may include any time limit the Court considers advisable.

(6) The Court may, on application, extend, vary or terminate an order under this Section.

(7) In determining whether to make an order under this Section and what order to make, the Court shall consider the following factors, if relevant:
   (a) the content of the intimate image or cyber-bullying;
   (b) the manner and repetition of the conduct;
   (c) the nature and extent of the harm caused;
   (d) the age and vulnerability of the person depicted in the intimate image distributed without consent or victim of cyber-bullying;
   (e) the purpose or intention of the person responsible for the distribution of the intimate image without consent or the cyber-bullying;
   (f) the occasion, context and subject-matter of the conduct;
   (g) the extent of the distribution of the intimate image or cyber-bullying;
   (h) the truth or falsity of the communication;
   (i) the conduct of the person responsible for the distribution of the intimate image or cyber-bullying, including any effort to minimize harm;
(j) the age and maturity of the person responsible for distribution of the intimate image without consent or cyber-bullying;
(k) the technical and operational practicalities and costs of carrying out the order;
(l) the Canadian Charter of Rights and Freedoms; and
(m) any other relevant factor or circumstance.

7. Defences

(1) In an application for an order respecting the distribution of an intimate image without consent or cyber-bullying under this Act, it is a defence for the respondent to show that the distribution of an intimate image without consent or communication is in the public interest and that the distribution or communication did not extend beyond what was in the public interest.

(2) In an application for an order respecting cyber-bullying under this Act, it is a defence for the respondent to show that
(a) the victim of the cyber-bullying expressly or by implication consented to the making of the communication;
(b) the publication of a communication was, in accordance with the rules of law relating to defamation,
   (i) fair comment on a matter of public interest,
   (ii) done in a manner consistent with principles of responsible journalism, or
   (iii) privileged;
(c) where the respondent is a peace officer acting in the course of the peace officer’s duties, that the communication was necessary to prevent a crime or discover, investigate or prosecute the perpetrators of a crime and did not extend beyond what was necessary;
(d) where the respondent is a public officer acting in the course of the duties of the public officer’s office, that the communication was necessary to fulfil the duties of that office and did not extend beyond what was necessary.

8. Publication ban for minors

(1) Subject to the regulations, where any person involved in a proceeding relating to an application made under Section 5 is a minor, no person shall publish or broadcast the name of that person, or any information likely to identify that person.

(2) In a proceeding to which subsection (1) applies, the Court shall identify the person by a pseudonym.

(3) For greater certainty, this Section continues to apply once the person is no longer a minor.

9. Publication ban where intimate image distributed

(1) Subject to the regulations, where an application is made under Section 5 respecting the distribution of an intimate image without consent and the applicant so requests, no person shall publish or broadcast the name of the applicant or any information likely to identify the applicant.

(2) In a proceeding to which subsection (1) applies, the Court shall identify the applicant by a pseudonym if the applicant requests to be so identified.

10. Additional right of action or remedy not barred

Applying for an order under this Act does not limit the right of a victim of cyber-bullying or a person depicted in an intimate image to pursue any right of action or remedy available to that person under common law or by statute.

11. Offence

A person who contravenes an order made under this Act, other than an order for payment of damages or accounting of profits, is guilty of an offence and liable on summary conviction to a fine of not more than $5,000 or to imprisonment for a term of not more than six months, or to both a fine and imprisonment.

12. Role of agency

(1) The Minister may establish or designate an agency to
   (a) provide public information and education regarding harmful on-line conduct;
   (b) advise public bodies on policies for on-line safety and conduct;
   (c) provide support and assistance to victims of intimate image distribution without consent and cyber-bullying;
   (d) provide information to victims of intimate image distribution without consent and cyber-bullying respecting the criminal justice system and proceedings under this Act;
   (e) provide information to victims of intimate image distribution without consent and cyber-bullying respecting contacting police;
A. Legislation on online harassment and cyber crimes cont

(f) provide voluntary dispute-resolution services, including advice, negotiation, mediation and restorative justice approaches in respect of harmful on-line conduct; and
(g) provide such other services, exercise such other powers and authorities and perform such other duties as may be prescribed by the regulations.

(2) The Minister may assign any of the functions and responsibilities of the agency to another person or organization on such terms and conditions as the Minister considers appropriate.

…

14. Review of Act

The Minister shall, within three years after this Act comes into force, undertake a review of its effectiveness in meeting its purposes and, within one year after the review is undertaken, table a report on the review in the Assembly if the Assembly is then sitting or, where it is not then sitting, file it with the Clerk of the Assembly.

Commonwealth Europe

UNITED KINGDOM
ENGLAND & WALES

Criminal Justice and Courts Act 2015

33. Disclosing private sexual photographs and films with intent to cause distress

(1) It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made-
(a) without the consent of an individual who appears in the photograph or film, and
(b) with the intention of causing that individual distress.

(2) But it is not an offence under this section for the person to disclose the photograph or film to the individual mentioned in subsection (1)(a) and (b).

(3) It is a defence for a person charged with an offence under this section to prove that he or she reasonably believed that the disclosure was necessary for the purposes of preventing, detecting or investigating crime.

(4) It is a defence for a person charged with an offence under this section to show that -
(a) the disclosure was made in the course of, or with a view to, the publication of journalistic material, and
(b) he or she reasonably believed that, in the particular circumstances, the publication of the journalistic material was, or would be, in the public interest.

(5) It is a defence for a person charged with an offence under this section to show that-
(a) he or she reasonably believed that the photograph or film had previously been disclosed for reward, whether by the individual mentioned in subsection (1)(a) and (b) or another person, and
(b) he or she had no reason to believe that the previous disclosure for reward was made without the consent of the individual mentioned in subsection (1)(a) and (b).

(6) A person is taken to have shown the matters mentioned in subsection (4) or (5) if -
(a) sufficient evidence of the matters is adduced to raise an issue with respect to it, and
(b) the contrary is not proved beyond reasonable doubt.

(7) For the purposes of subsections (1) to (5) -
(a) “consent” to a disclosure includes general consent covering the disclosure, as well as consent to the particular disclosure, and
(b) “publication” of journalistic material means disclosure to the public at large or to a section of the public.

(8) A person charged with an offence under this section is not to be taken to have disclosed a photograph or film with the intention of causing distress merely because that was a natural and probable consequence of the disclosure.
(9) A person guilty of an offence under this section is liable -
   (a) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both), and
   (b) on summary conviction, to imprisonment for a term not exceeding 12 months or a fine (or both).

(10) Schedule 8 makes special provision in connection with the operation of this section in relation to persons providing
     information society services.

(11) In relation to an offence committed before section 154(1) of the Criminal Justice Act 2003 comes into force,
     the reference in subsection (9)(b) to 12 months is to be read as a reference to 6 months.

(12) In relation to an offence committed before section 85 of the Legal Aid, Sentencing and Punishment of Offenders Act
     2012 comes into force, the reference in subsection (9)(b) to a fine is to be read as a reference to a fine not exceeding
     the statutory maximum.

34. Meaning of “disclose” and “photograph or film”

(1) The following apply for the purposes of section 33, this section and section 35.

(2) A person “discloses” something to a person if, by any means, he or she gives or shows it to the person or makes
    it available to the person.

(3) Something that is given, shown or made available to a person is disclosed—
    (a) whether or not it is given, shown or made available for reward, and
    (b) whether or not it has previously been given, shown or made available to the person.

(4) “Photograph or film” means a still or moving image in any form that—
    (a) appears to consist of or include one or more photographed or filmed images, and
    (b) in fact consists of or includes one or more photographed or filmed images.

(5) The reference in subsection (4)(b) to photographed or filmed images includes photographed or filmed images
    that have been altered in any way.

(6) “Photographed or filmed image” means a still or moving image that—
    (a) was originally captured by photography or filming, or
    (b) is part of an image originally captured by photography or filming.

(7) “Filming” means making a recording, on any medium, from which a moving image may be produced by any means.

(8) References to a photograph or film include -
    (a) a negative version of an image described in subsection (4), and
    (b) data stored by any means which is capable of conversion into an image described in subsection (4).

35. Meaning of “private” and “sexual”

(1) The following apply for the purposes of section 33.

(2) A photograph or film is “private” if it shows something that is not of a kind ordinarily seen in public.

(3) A photograph or film is “sexual” if—
    (a) it shows all or part of an individual’s exposed genitals or pubic area,
    (b) it shows something that a reasonable person would consider to be sexual because of its nature, or
    (c) its content, taken as a whole, is such that a reasonable person would consider it to be sexual.

(4) Subsection (5) applies in the case of -
    (a) a photograph or film that consists of or includes a photographed or filmed image that has been altered in any way,
    (b) a photograph or film that combines two or more photographed or filmed images, and
    (c) a photograph or film that combines a photographed or filmed image with something else.

(5) The photograph or film is not private and sexual if—
    (a) it does not consist of or include a photographed or filmed image that is itself private and sexual,
    (b) it is only private or sexual by virtue of the alteration or combination mentioned in subsection (4), or
    (c) it is only by virtue of the alteration or combination mentioned in subsection (4) that the person mentioned in section
       33(1)(a) and (b) is shown as part of, or with, whatever makes the photograph or film private and sexual.
A. Legislation on online harassment and cyber crimes cont

Commonwealth Pacific

AUSTRALIA
QUEENSLAND

Criminal Code 1989 (as amended)
Chapter 22 Offences against morality
207A Definitions for this chapter

In this chapter-

... 

distribute includes-
(a) communicate, exhibit, send, supply or transmit to someone, whether to a particular person or not; and
(b) make available for access by someone, whether by a particular person or not; and
(c) enter into an agreement or arrangement to do something in paragraph (a) or (b); and
(d) attempt to distribute.

... 

intimate image, of a person-
(a) means a moving or still image that depicts-
(i) the person engaged in an intimate sexual activity that is not ordinarily done in public; or
(ii) the person's genital or anal region, when it is bare or covered only by underwear; or
(iii) if the person is female or a transgender or intersex person who identifies as female- the person's bare breasts; and
(b) includes an image that has been altered to appear to show any of the things mentioned in paragraph (a)(i) to (iii); and
(c) includes an image depicting a thing mentioned in paragraph (a)(i) to (iii), even if the thing has been digitally obscured, if the person is depicted in a sexual way.

material includes anything that contains data from which text, images or sound can be generated.

network, of computers or other devices, includes part of a network of computers or other devices.

observe means observe by any means. private act, for a person, means-
(a) showering or bathing; or
(b) using a toilet; or
(c) another activity when the person is in a state of undress; or
(d) intimate sexual activity that is not ordinarily done in public.

private place means a place where a person might reasonably be expected to be engaging in a private act.

prohibited visual recording, of a person, means-
(a) a visual recording of the person, in a private place or engaging in a private act, made in circumstances where a reasonable adult would expect to be afforded privacy; or
(b) a visual recording of the person's genital or anal region, when it is bare or covered only by underwear, made in circumstances where a reasonable adult would expect to be afforded privacy in relation to that region.

someone, in the context of a description or depiction, includes the body parts of someone, including for example, someone's breast or genitalia.

state of undress, for a person, means-
(a) the person is naked or the person's genital or anal region is bare or, if the person is female or a transgender or intersex person who identifies as female, the person's breasts are bare; or
(b) the person is wearing only underwear; or
(c) the person is wearing only some outer garments so that some of the person's underwear is not covered by an outer garment.

visually record, a person, means record, or transmit, by any means, moving or still images of the person or part of the person.
...
223 Distributing intimate images

(1) A person who distributes an intimate image of another person—
(a) without the other person’s consent; and
(b) in a way that would cause the other person distress reasonably arising in all the circumstances;

commits a misdemeanour.

Examples of circumstances for subsection (1)(b)—
• the circumstances surrounding the distribution of the intimate image
• the extent to which the distribution of the intimate image interferes with the other person’s privacy
• the relationship, if any, between the person who distributes the intimate image and the other person

Maximum penalty—3 years imprisonment.

(2) For subsection (1)(a), a child under the age of 16 years is incapable of giving consent.

(3) For subsection (1)(b), it is immaterial whether the person who distributes the intimate image intends to cause, or actually causes, the other person distress.

(4) It is a defence to a charge of an offence against subsection (1) to prove that—
(a) the person engaged in the conduct that is alleged to constitute the offence for a genuine artistic, educational, legal, medical, scientific or public benefit purpose; and
(b) the person’s conduct was, in the circumstances, reasonable for that purpose.

(5) In this section—
consent means consent freely and voluntarily given by a person with the cognitive capacity to give the consent.

227A Observations or recordings in breach of privacy

(1) A person who observes or visually records another person, in circumstances where a reasonable adult would expect to be afforded privacy—
(a) without the other person’s consent; and (b) when the other person—
(i) is in a private place; or
(ii) is engaging in a private act and the observation or visual recording is made for the purpose of observing or visually recording a private act; commits a misdemeanour.

Maximum penalty—3 years imprisonment.

Examples of circumstances where a reasonable adult would expect to be afforded privacy—

1. A person changing in a communal change room at a swimming pool may expect to be observed by another person who is also changing in the room but may not expect to be visually recorded

2. A person who needs help to dress or use a toilet may expect to be observed by the person giving the help but may not expect to be observed by another person.

(2) A person who observes or visually records another person’s genital or anal region, in circumstances where a reasonable adult would expect to be afforded privacy in relation to that region—
(a) without the other person’s consent; and
(b) when the observation or visual recording is made for the purpose of observing or visually recording the other person’s genital or anal region; commits a misdemeanour.

Maximum penalty—3 years imprisonment.

Example for subsection (2)—
using a mobile phone in a public place to take photos of women’s underwear under their skirts without their consent.

(3) In this section—
consent means consent freely and voluntarily given by a person with the cognitive capacity to give the consent.

genital or anal region, of a person, means the person’s genital or anal region when it is bare or covered only by underwear.
A. Legislation on online harassment and cyber crimes cont

227B Distributing prohibited visual recordings

(1) A person who distributes a prohibited visual recording of another person having reason to believe it to be a prohibited visual recording, without the other person’s consent, commits a misdemeanour.
Maximum penalty—3 years imprisonment.

(2) In this section—
consent means consent freely and voluntarily given by a person with the cognitive capacity to give the consent.

229A Threats to distribute intimate image or prohibited visual recording

(1) A person commits a misdemeanour if—
(a) the person makes a threat to another person to distribute an intimate image or prohibited visual recording of the other person—
(i) without the other person’s consent; and
(ii) in a way that would cause the other person distress reasonably arising in all the circumstances; and
(b) the threat is made in a way that would cause the other person fear, reasonably arising in all the circumstances, of the threat being carried out.
Examples of circumstances for subsection (1)—
• the circumstances surrounding the threat
• the relationship, if any, between the person who makes the threat and the other person
Maximum penalty—3 years imprisonment.

(2) A person commits a misdemeanour if—
(a) the person makes a threat to another person (person A) to distribute an intimate image or prohibited visual recording of another person (person B)—
(i) without person B’s consent; and
(ii) in a way that would cause either person A or person B distress reasonably arising in all the circumstances; and
(b) the threat is made in a way that would cause person A fear, reasonably arising in all the circumstances, of the threat being carried out.
Examples of circumstances for subsection (2)—
• the circumstances surrounding the threat
• the relationship, if any, between the person who makes the threat and person A or person B
Maximum penalty—3 years imprisonment.

(3) For subsections (1) and (2) it is immaterial whether—
(a) the intimate image or prohibited visual recording exists or does not exist; or
(b) the person who makes the threat intends to cause, or actually causes, the fear mentioned in the subsection.

(4) For subsections (1)(a)(i) and (2)(a)(i), a child under the age of 16 years is incapable of giving consent.

(5) In this section—
consent means consent freely and voluntarily given by a person with the cognitive capacity to give the consent.

229AA Rectification order—offence against s 223, 227A, 227B or 229A

(1) If a person is convicted of an offence against section 223(1), 227A(1) or (2), 227B(1) or 229A(1) or (2) the court may order the person to take reasonable action to remove, retract, recover, delete or destroy an intimate image or prohibited visual recording involved in the offence within a stated period.

(2) A person who fails to comply with an order made under subsection (1) commits a misdemeanour.
Maximum penalty—2 years imprisonment.

NEW SOUTH WALES

Crimes Act 1900 (as amended by the Crimes (Domestic and Personal Violence) Act 2007)

Division 15C Recording and distributing intimate images

91N. Definitions

(1) In this Division:
distribute includes:
(a) send, supply, exhibit, transmit or communicate to another person, or
(b) make available for viewing or access by another person, whether in person or by electronic, digital or any other means.
engaged in a private act means:
(a) in a state of undress, or
(b) using the toilet, showering or bathing, or
(c) engaged in a sexual act of a kind not ordinarily done in public, or
(d) engaged in any other like activity.

image means a still or moving image, whether or not altered.

intimate image means:
(a) an image of a person’s private parts, or of a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, or
(b) an image that has been altered to appear to show a person’s private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy.

private parts means:
(a) a person’s genital area or anal area, whether bare or covered by underwear, or
(b) the breasts of a female person, or transgender or intersex person identifying as female, whether or not the breasts are sexually developed.

record an image means record, take or capture an image, by any means.

(2) A person may be regarded as having distributed an image to another person whether or not the other person views or accesses the image.

91O. Meaning of consent in intimate image offences

(1) This section applies to all offences under this Division.

(2) A person consents to the recording of an intimate image if the person freely and voluntarily agrees to the recording of the intimate image.

(3) A person consents to the distribution of an intimate image if the person freely and voluntarily agrees to the distribution of the intimate image.

(4) A person who consents to the recording or distribution of an image on a particular occasion is not, by reason only of that fact, to be regarded as having consented to the recording or distribution of that image or any other image on another occasion.

(5) A person who consents to the distribution of an image to a particular person or in a particular way is not, by reason only of that fact, to be regarded as having consented to the distribution of that image or any other image to another person or in another way.

(6) A person who distributes an image of himself or herself is not, by reason only of that fact, to be regarded as having consented to any other distribution of the image.

(7) A person does not consent to the recording or distribution of an intimate image:
(a) if the person is under the age of 16 years or does not otherwise have the capacity to consent, including because of cognitive incapacity, or
(b) if the person does not have the opportunity to consent because the person is unconscious or asleep, or
(c) if the person consents because of threats of force or terror (whether the threats are against, or the terror is instilled in, that person or any other person), or
(d) if the person consents because the person is unlawfully detained.

(8) This section does not limit the grounds on which it may be established that a person does not consent to the recording or distribution of an intimate image.

91P. Record intimate image without consent

(1) A person who intentionally records an intimate image of another person:
(a) without the consent of the person, and
(b) knowing the person did not consent to the recording or being reckless as to whether the person consented to the recording, is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 3 years, or both.

(2) A prosecution of a person under the age of 16 years for an offence against this section is not to be commenced without the approval of the Director of Public Prosecutions.
A. Legislation on online harassment and cyber crimes cont

91Q. Distribute intimate image without consent

1. A person who intentionally distributes an intimate image of another person:
   (a) without the consent of the person, and
   (b) knowing the person did not consent to the distribution or being reckless as to whether the person consented
to the distribution, is guilty of an offence.
   Maximum penalty: 100 penalty units or imprisonment for 3 years, or both.

2. A prosecution of a person under the age of 16 years for an offence against this section is not to be commenced
   without the approval of the Director of Public Prosecutions.

91R. Threaten to record or distribute intimate image

1. A person who threatens to record an intimate image of another person:
   (a) without the consent of the other person, and
   (b) intending to cause that other person to fear that the threat will be carried out, is guilty of an offence.
   Maximum penalty: 100 penalty units or imprisonment for 3 years, or both.

2. A person who threatens to distribute an intimate image of another person:
   (a) without the consent of the other person, and
   (b) intending to cause that other person to fear that the threat will be carried out, is guilty of an offence.
   Maximum penalty: 100 penalty units or imprisonment for 3 years, or both.

3. A threat may be made by any conduct, and may be explicit or implicit and conditional or unconditional.

4. A person may threaten to distribute an image whether or not the image exists.

5. In proceedings for an offence against this section, the prosecution is not required to prove that the person alleged
to have been threatened actually feared that the threat would be carried out.

6. A prosecution of a person under the age of 16 years for an offence against this section is not to be commenced
   without the approval of the Director of Public Prosecutions.

91S. Court may order rectification

1. A court that finds a person guilty of an offence against section 91P or 91Q may order the person to take reasonable
   actions to remove, retract, recover, delete or destroy any intimate image recorded or distributed by the person
   in contravention of the section within a period specified by the court.

2. A person who, without reasonable excuse, contravenes an order made under this section is guilty of an offence.
   Maximum penalty: 50 penalty units or imprisonment for 2 years, or both.

3. An offence against this section is a summary offence.

91T. Exceptions

1. A person does not commit an offence against section 91P or 91Q if:
   (a) the conduct alleged to constitute the offence was done for a genuine medical or scientific purpose, or
   (b) the conduct alleged to constitute the offence was done by a law enforcement officer for a genuine law enforcement
       purpose, or
   (c) the conduct alleged to constitute the offence was required by a court or otherwise reasonably necessary to be done
       for the purpose of legal proceedings, or
   (d) a reasonable person would consider the conduct of the accused person acceptable, having regard to each
       of the following (to the extent relevant):
       (i) the nature and content of the image,
       (ii) the circumstances in which the image was recorded or distributed,
       (iii) the age, intellectual capacity, vulnerability or other relevant circumstances of the person depicted in the image,
       (iv) the degree to which the accused person’s actions affect the privacy of the person depicted in the image,
       (v) the relationship between the accused person and the person depicted in the image.

2. In this section: law enforcement officer means a police officer or other person who exercises law enforcement
functions under a law of this State, another State, a Territory or the Commonwealth.
NEW ZEALAND

Harmful Digital Communications Act 2015

3. Purpose

The purpose of this Act is to-
(a) deter, prevent, and mitigate harm caused to individuals by digital communications; and
(b) provide victims of harmful digital communications with a quick and efficient means of redress.

4. Interpretation

In this Act, unless the context otherwise requires-

... digital communication-
(a) means any form of electronic communication; and
(b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.

harm means serious emotional distress.

... intimate visual recording-
(a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the individual who is the subject of the recording, and that is of—
(i) an individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is—
(A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or
(B) engaged in an intimate sexual activity; or
(C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or
(ii) an individual’s naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made—
(A) from beneath or under an individual’s clothing; or
(B) through an individual’s outer clothing in circumstances where it is unreasonable to do so; and
(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in—
(i) a physical form; or
(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing.

... online content host, in relation to a digital communication, means the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user.

posts a digital communication-
(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication—
(i) any information, whether truthful or untruthful, about the victim; or
(ii) an intimate visual recording of another individual; and
(b) includes an attempt to do anything referred to in paragraph (a).
A. Legislation on online harassment and cyber crimes  cont

6. Communication principles

(1) The communication principles are-

**Principle 1**
A digital communication should not disclose sensitive personal facts about an individual.

**Principle 2**
A digital communication should not be threatening, intimidating, or menacing.

**Principle 3**
A digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.

**Principle 4**
A digital communication should not be indecent or obscene.

**Principle 5**
A digital communication should not be used to harass an individual.

**Principle 6**
A digital communication should not make a false allegation.

**Principle 7**
A digital communication should not contain a matter that is published in breach of confidence.

**Principle 8**
A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.

**Principle 9**
A digital communication should not incite or encourage an individual to commit suicide.

**Principle 10**
A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

…

8. Functions and powers of Approved Agency

(1) The functions of the Approved Agency are—

(a) to receive and assess complaints about harm caused to individuals by digital communications:
(b) to investigate complaints:
(c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
(d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act:
(e) to provide education and advice on policies for online safety and conduct on the Internet:
(f) to perform the other functions conferred on it by or under this Act, including functions prescribed by Order in Council made under section 7.

(2) The Agency may, subject to any other enactment, seek and receive any information that the Agency considers will assist it in the performance of its functions.

(3) The Agency may refuse to investigate, or cease investigating, any complaint if the Agency considers that—

(a) the complaint is trivial, frivolous, or vexatious; or
(b) the subject matter or nature of the complaint is unlikely to cause harm to any individual; or
(c) the subject matter or nature of the complaint does not contravene the communication principles.

(4) The Agency may decide not to take any further action on a complaint if, in the course of assessing or investigating the complaint, it appears to the Agency that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(5) If the Agency decides not to take any further action on a complaint, it must notify the complainant of the right to apply to the District Court for an order under this Act.

…
11. Who may bring proceedings

(1) Any of the following may apply to the District Court for an order under section 18 or 19:
   (a) an individual (the affected individual) who alleges that he or she has suffered or will suffer harm as a result of a digital communication;
   (b) a parent or guardian on behalf of the affected individual;
   (c) the professional leader of a registered school or his or her delegate, if the affected individual is a student of that school and consents to the professional leader or delegate bringing the proceedings;
   (d) the Police, if the digital communication constitutes a threat to the safety of an individual.

12. Threshold for proceedings

(1) An applicant referred to in section 11(1)(a), (b), or (c) may not apply for an order under section 18 or 19 in respect of a digital communication unless the Approved Agency has first received a complaint about the communication and had a reasonable opportunity to assess the complaint and decide what action (if any) to take.

(2) In any case, the District Court must not grant an application from an applicant referred to in section 11(1)(a), (b), or (c) for an order under section 18 or 19 unless it is satisfied that-
   (a) there has been a threatened serious breach, a serious breach, or a repeated breach of 1 or more communication principles; and
   (b) the breach has caused or is likely to cause harm to an individual.

(3) The court may, on its own initiative, dismiss an application from an applicant referred to in section 11(1)(a), (b), or (c) without a hearing if it considers that the application is frivolous or vexatious, or for any other reason does not meet the threshold in subsection (2).

(4) The court may, on its own initiative, dismiss an application under section 11 from the Police if satisfied that, having regard to all the circumstances of the case, the application should be dismissed.

19. Orders that may be made by court

(1) The District Court may, on an application, make 1 or more of the following orders against a defendant:
   (a) an order to take down or disable material:
   (b) an order that the defendant cease or refrain from the conduct concerned:
   (c) an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual:
   (d) an order that a correction be published:
   (e) an order that a right of reply be given to the affected individual:
   (f) an order that an apology be published.

(2) The District Court may, on an application, make 1 or more of the following orders against an online content host:
   (a) an order to take down or disable public access to material that has been posted or sent:
   (b) an order that the identity of the author of an anonymous or pseudonymous communication be released to the court:
   (c) an order that a correction be published in any manner that the court specifies in the order:
   (d) an order that a right of reply be given to the affected individual in any manner that the court specifies in the order.

(3) The District Court may, on application, make an order against an IPAP [Internet protocol address provider] that the identity of an anonymous communicator be released to the court.

(4) The court may also do 1 or more of the following:
   (a) make a direction applying an order provided for in subsection (1) or (2) to other persons specified in the direction, if there is evidence that those others have been encouraged to engage in harmful digital communications towards the affected individual:
   (b) make a declaration that a communication breaches a communication principle:
   (c) order that the names of any specified parties be suppressed.

(5) In deciding whether or not to make an order, and the form of an order, the court must take into account the following:
   (a) the content of the communication and the level of harm caused or likely to be caused by it:
   (b) the purpose of the communicator, in particular whether the communication was intended to cause harm:
   (c) the occasion, context, and subject matter of the communication:
   (d) the extent to which the communication has spread beyond the original parties to the communication:
A. Legislation on online harassment and cyber crimes cont

(e) the age and vulnerability of the affected individual:
(f) the truth or falsity of the statement:
(g) whether the communication is in the public interest:
(h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused:
(i) the conduct of the affected individual or complainant:
(j) the technical and operational practicalities, and the costs, of an order:
(k) the appropriate individual or other person who should be subject to the order.

(6) In doing anything under this section, the court must act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

…

21. Offence of non-compliance with order

(1) A person who, without reasonable excuse, fails to comply with an order made under section 18 or 19 commits an offence.

(2) A person who commits an offence against this section is liable on conviction to,—
   (a) in the case of a natural person, imprisonment for a term not exceeding 6 months or a fine not exceeding $5,000:
   (b) in the case of a body corporate, a fine not exceeding $20,000.

22. Causing harm by posting digital communication

(1) A person commits an offence if-
   (a) the person posts a digital communication with the intention that it cause harm to a victim; and
   (b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
   (c) posting the communication causes harm to the victim.

(2) In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including-
   (a) the extremity of the language used:
   (b) the age and characteristics of the victim:
   (c) whether the digital communication was anonymous:
   (d) whether the digital communication was repeated:
   (e) the extent of circulation of the digital communication:
   (f) whether the digital communication is true or false:
   (g) the context in which the digital communication appeared.

(3) A person who commits an offence against this section is liable on conviction to,—
   (a) in the case of a natural person, imprisonment for a term not exceeding 2 years or a fine not exceeding $50,000:
   (b) in the case of a body corporate, a fine not exceeding $200,000.

(4) In this section, victim means the individual who is the target of a posted digital communication.

…

23. Liability of online content host for content posted by user

(1) Section 24 provides protection for an online content host in respect of any specific content of a digital communication posted by a person and hosted by the online content host if the host follows the process in that section.

(2) The fact that an online content host does not take advantage of section 24 does not of itself create any civil or criminal liability for hosting the specific content.

(3) Section 24 does not affect any rights or defences otherwise available to the online content host in respect of the hosting of the specific content (for example, the removal of content or the creation, exercise, or taking advantage of any contractual indemnity or immunity or any other term of use).

(4) This section is subject to section 25(5).

24. Process for obtaining protection against liability for specific content

(1) No civil or criminal proceedings may be brought against an online content host in respect of the content complained of (the specific content) if the online content host-
   (a) receives a notice of complaint about the specific content; and
   (b) complies with subsection (2).
(2) The requirements of this subsection are that-

Host to notify author of complaint

(a) the online content host must, as soon as practicable but no later than 48 hours after receiving a notice of complaint,-

(i) provide the author of the specific content with a copy of the notice of complaint, altered to conceal personal information that identifies the complainant if the host has received confirmation that the complainant does not consent to the host providing that information to the author; and

(ii) notify the author that the author may submit a counter-notice to the host within 48 hours after receiving that notification:

(b) if the host is unable to contact the author (for example, because the identity of the author is unknown) after taking reasonable steps to do so, the host must take down or disable the specific content as soon as practicable after taking those steps but no later than 48 hours after receiving a notice of complaint:

Author’s counter-notice consenting to removal of content

(c) if the author submits a valid counter-notice no later than 48 hours after receiving the host’s notification under paragraph (a) in which the author consents to the removal of the specific content, the host must take down or disable the specific content as soon as practicable after receiving that counter-notice:

Author’s counter-notice refusing consent to removal of content

(d) if the author submits a valid counter-notice no later than 48 hours after receiving the host’s notification under paragraph (a) in which the author refuses to consent to the removal of the specific content, the host must leave the specific content in place and, as soon as practicable after receiving that counter-notice,—

(i) notify the complainant of the author’s decision; and

(ii) if the author consents, provide the complainant with personal information that identifies the author:

Author failing to submit valid counter-notice

(e) if the author does not submit a valid counter-notice in accordance with this subsection (whether by failing to submit a counter-notice or by submitting an invalid counter-notice), the host must take down or disable the specific content as soon as practicable but no later than 48 hours after notifying the author under paragraph (a).

(3) A notice of complaint must-

(a) state the complainant’s name and a telephone number, a physical address, and an email address for the complainant; and

(b) state the specific content, and explain why the complainant considers that the specific content-

(i) is unlawful; or

(ii) breaches 1 or more communication principles and has caused harm; and

(c) sufficiently enable the specific content to be readily located; and

(d) state whether the complainant consents to personal information that identifies the complainant being released to the author; and

(e) contain any other information that the complainant considers relevant.

(4) A counter-notice must state-

(a) the author’s name and a telephone phone number, a physical address, and an email address for the author; and

(b) whether the author consents to personal information that identifies the author being released to the complainant; and

(c) whether the author consents to the removal of the specific content.

(5) An online content host must not disclose any personal information about the complainant or author under privacy principle 11(e)(iv) in section 6 of the Privacy Act 1993, except by order of a District Court Judge or a High Court Judge made on an application under this subsection.

(6) Nothing in subsection (5) affects the application of any other provision in the Privacy Act 1993.

(7) This section is subject to section 25(5).

25. Further provisions related to section 24

(1) The Approved Agency may lodge a notice of complaint under section 24 on behalf of a complainant and provide advice and assistance to the complainant in relation to the complaint.

(2) The protection conferred on an online content host by section 24 does not apply if the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content in the manner provided in that section.
A. Legislation on online harassment and cyber crimes cont

(3) The protection conferred on an online content host by section 24 does not apply if the person who provides the specific content does so on behalf, or at the direction, of the online content host.

…

(5) Nothing in section 23 or 24 or this section limits the right of an individual to injunctive relief in relation to the content of a digital communication posted by another person and hosted by the online content host.

United States of America

National Conference of Commissioners on Uniform State Laws
Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act 2018

SECTION 1. SHORT TITLE
This [act] may be cited as the Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act.

SECTION 2. DEFINITIONS
In this [act]:

(1) “Consent” means affirmative, conscious, and voluntary authorization by an individual with legal capacity to give authorization.

(2) “Depicted individual” means an individual whose body is shown in whole or in part in an intimate image.

(3) “Disclosure” means transfer, publication, or distribution to another person. “Disclose” has a corresponding meaning.

(4) “Identifiable” means recognizable by a person other than the depicted individual:
   (A) from an intimate image itself; or
   (B) from an intimate image and identifying characteristic displayed in connection with the intimate image.

(5) “Identifying characteristic” means information that may be used to identify a depicted individual

(6) “Individual” means a human being.

(7) “Intimate image” means a photograph, film, video recording, or other similar medium that shows:
   (A) the uncovered genitals, pubic area, anus, or female post-pubescent nipple of a depicted individual; or
   (B) a depicted individual engaging in or being subjected to sexual conduct.

(8) “Person” means an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

(9) “Sexual conduct” includes:
   (A) masturbation;
   (B) genital, anal, or oral sex;
   (C) sexual penetration of, or with, an object;
   (D) bestiality; or
   (E) the transfer of semen onto a depicted individual.

…

SECTION 3. CIVIL ACTION

(a) In this section:
   (1) “Harm” includes physical harm, economic harm, and emotional distress whether or not accompanied by physical or economic harm.
   (2) “Private” means:
      (A) created or obtained under circumstances in which a depicted individual had a reasonable expectation of privacy; or
      (B) made accessible through [theft, bribery, extortion, fraud, false pretenses, voyeurism, or exceeding authorized access to an account, message, file, device, resource, or property].
(b) Except as otherwise provided in Section 4, a depicted individual who is identifiable and who suffers harm from a person’s intentional disclosure or threatened disclosure of an intimate image that was private without the depicted individual’s consent has a cause of action against the person if the person knew [or acted with reckless disregard for whether]:

(1) the depicted individual did not consent to the disclosure;
(2) the intimate image was private; and
(3) the depicted individual was identifiable.

(c) The following conduct by a depicted individual does not establish by itself that the individual consented to the disclosure of the intimate image which is the subject of an action under this [act] or that the individual lacked a reasonable expectation of privacy:

(1) consent to creation of the image; or
(2) previous consensual disclosure of the image.

(d) A depicted individual who does not consent to the sexual conduct or uncovering of the part of the body depicted in an intimate image of the individual retains a reasonable expectation of privacy even if the image was created when the individual was in a public place.

…

SECTION 4. EXCEPTIONS TO LIABILITY

(a) In this section:

(1) “Child” means an unemancipated individual who is less than [18] years of age.
(2) “Parent” means an individual recognized as a parent under law of this state other than this [act].

(b) A person is not liable under this [act] if the person proves that disclosure of, or a threat to disclose, an intimate image was:

(1) made in good faith in
(A) law enforcement;
(B) a legal proceeding; or
(C) medical education or treatment;
(2) made in good faith in the reporting or investigation of:
(A) unlawful conduct; or
(B) unsolicited and unwelcome conduct;
(3) related to a matter of public concern or public interest; or
(4) reasonably intended to assist the depicted individual.

(c) Subject to subsection (d), a defendant who is a parent, legal guardian, or [individual with legal custody] of a child is not liable under this [act] for a disclosure or threatened disclosure of an intimate image, as defined in Section 2(7)(A), of the child.

(d) If a defendant asserts an exception to liability under subsection (c), the exception does not apply if the plaintiff proves the disclosure was:

(1) prohibited by law other than this [act]; or
(2) made for the purpose of sexual arousal, sexual gratification, humiliation, degradation, or monetary or commercial gain.

(e) Disclosure of, or a threat to disclose, an intimate image is not a matter of public concern or public interest solely because the depicted individual is a public figure.

…

SECTION 5. PLAINTIFF’S PRIVACY

Alternative A
In an action under this [act] a plaintiff may proceed using a pseudonym in place of the true name of the plaintiff under [applicable state law or procedural rule].

Alternative B
In an action under this [act]:

(1) the court may exclude or redact from all pleadings and documents filed in the action other identifying characteristics of the plaintiff under [applicable state law or procedural rule];
(2) a plaintiff to whom paragraph (1) applies shall file with the court and serve on the defendant a confidential information form that includes the excluded or redacted plaintiff’s name and other identifying characteristics; and
(3) the court may make further orders as necessary to protect the identity and privacy of a plaintiff.

End of Alternatives
A. Legislation on online harassment and cyber crimes cont

... SECTION 6. REMEDIES

(a) In an action under this [act], a prevailing plaintiff may recover:
   (1) the greater of:
      (A) economic and noneconomic damages proximately caused by the defendant’s disclosure or threatened disclosure, including damages for emotional distress whether or not accompanied by other damages; or
      (B) statutory damages not to exceed $[10,000] against each defendant found liable under this [act] for all disclosures and threatened disclosures by the defendant of which the plaintiff knew or reasonably should have known when filing the action or which became known during the pendency of the action. In determining the amount of statutory damages under subsection (a)(1)(B), consideration must be given to the age of the parties at the time of the disclosure or threatened disclosure, the number of disclosures or threatened disclosures made by the defendant, the breadth of distribution of the image by the defendant, and other exacerbating or mitigating factors;
   (2) an amount equal to any monetary gain made by the defendant from disclosure of the intimate image; and
   (3) punitive damages [as allowed under law of this state other than this [act]].

(b) In an action under this [act], the court may award a prevailing plaintiff:
   (1) reasonable attorney’s fees [and costs]; and
   (2) additional relief, including injunctive relief.

(c) This [act] does not affect a right or remedy available under law of this state other than this [act].

International & Regional Conventions

African Union Convention on Cyber Security and Personal Data Protection 2014

Article 29: Offences specific to Information and Communication Technologies

... 3. Content related offences

1. State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:
   a) Produce, register, offer, manufacture, make available, disseminate and transmit an image or a representation of child pornography through a computer system;
   b) Procure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system;
   c) Possess an image or representation of child pornography in a computer system or on a computer data storage medium;
   d) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor;
   e) Create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system;
   f) Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics;
   g) Insult, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion or political opinion, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics;
   h) Deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system.

2. State Parties shall take the necessary legislative and/or regulatory measures to make the offences provided for under this Convention criminal offences. When such offences are committed under the aegis of a criminal organization, they will be punishable by the maximum penalty prescribed for the offense.
3. State Parties shall take the necessary legislative and/or regulatory measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of the materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in this Convention.

Article 31: Adapting certain sanctions to Information and Communication Technologies

2. Other criminal sanctions

a) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offense committed through a digital communication medium, the competent court may hand down additional sanctions;

b) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offence committed through a digital communication medium, the judge may in addition order the mandatory dissemination, at the expense of the convicted person, of an extract of the decision, through the same medium, and according to modalities prescribed by the law of Member States;

SADC Model Law on Computer Crime and Cybercrime 2013

20. Disclosure of details of an investigation

An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses:

(a) the fact that an order has been made; or
(b) anything done under the order; or
(c) any data collected or recorded under the order;
 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

22. Harassment utilizing means of electronic communication

A person who initiates any electronic communication with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behaviour, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

27. Production Order

If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement officer] [police officer] that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that:

(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or
(b) an Internet service provider in [enacting country] to [sic] produce information about persons who subscribe to or otherwise use the service.

31. Interception of content data

(1) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate][may] [shall]:

(b)[sic] order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or
A. Legislation on online harassment and cyber crimes cont

32. Forensic Tool

(1) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate][may][shall] authorize a [law enforcement] [police] officer to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect’s computer system in order to collect the relevant evidence. The application needs to contain the following information:

(a) suspect of the offence, if possible with name and address, and

(b) description of the targeted computer system, and

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

...

(6) If necessary a police officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.

...

33. No Monitoring Obligation

When providing the services contemplated in this Chapter there is no general obligation on an Internet service provider to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

The [Minister] may, subject to the provisions of any other law, prescribe procedures for service providers to

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.
B. Related legislation: Voyeurism

Commonwealth Pacific

AUSTRALIA
NEW SOUTH WALES

Crimes Act 1900
Division 15B - Voyeurism and related offences

91I. Definitions
(1) In this Division:

building includes a vehicle, vessel, tent or temporary structure.

private parts means:
   (a) a person’s genital area or anal area, whether bare or covered by underwear, or
   (b) the breasts of a female person, or transgender or intersex person identifying as female, whether or not the breasts
       are sexually developed.

(2) For the purposes of this Division, a person is engaged in a private act if:
   (a) the person is in a state of undress, using the toilet, showering or bathing, engaged in a sexual act of a kind not
       ordinarily done in public, or engaged in any other like activity, and
   (b) the circumstances are such that a reasonable person would reasonably expect to be afforded privacy.

(3) For the purposes of this Division, a person films another person, or another person’s private parts, if the person causes
    one or more images (whether still or moving) of the other person or the other person’s private parts to be recorded
    or transmitted for the purpose of enabling the person or a third person to observe those images (whether during the
    filming or later).

91J. Voyeurism

General offence
(1) A person who, for the purpose of obtaining sexual arousal or sexual gratification, observes a person who is engaged
    in a private act:
    (a) without the consent of the person being observed to being observed for that purpose, and
    (b) knowing that the person being observed does not consent to being observed for that purpose,
    is guilty of an offence.
    Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

(2) An offence against subsection (1) is a summary offence.

Aggravated offence
(3) A person who, for the purpose of obtaining sexual arousal or sexual gratification, observes a person who is engaged
    in a private act:
    (a) without the consent of the person being observed to being observed for that purpose, and
    (b) knowing that the person being observed does not consent to being observed for that purpose, and
    (c) in circumstances of aggravation,
    is guilty of an offence.
    Maximum penalty: imprisonment for 5 years.
B. Related legislation: Voyeurism cont

(4) In this section, *circumstances of aggravation* means circumstances in which:
   (a) the person whom the offender observed was a child under the age of 16 years, or
   (b) the offender constructed or adapted the fabric of any building for the purpose of facilitating the commission of the offence.

Alternative verdict

(5) If on the trial of a person charged with an offence against subsection (3) the trier of fact is not satisfied that the offence is proven but is satisfied that the person has committed an offence against subsection (1), the trier of fact may acquit the person of the offence charged and find the person guilty of an offence against subsection (1). The person is liable to punishment accordingly.

Attempts

(6) A person who attempts to commit an offence under subsection (1) or (3) is liable to the penalty provided for the commission of the offence.

91K. Filming a person engaged in private act

General offence

(1) A person who, for the purpose of obtaining, or enabling another person to obtain, sexual arousal or sexual gratification, films another person who is engaged in a private act:
   (a) without the consent of the person being filmed to being filmed for that purpose, and
   (b) knowing that the person being filmed does not consent to being filmed for that purpose,
   is guilty of an offence.
   Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

(2) An offence against subsection (1) is a summary offence.

Aggravated offence

(3) A person who, for the purpose of obtaining, or enabling another person to obtain, sexual arousal or sexual gratification, films another person who is engaged in a private act:
   (a) without the consent of the person being filmed to being filmed for that purpose, and
   (b) knowing that the person being filmed does not consent to being filmed for that purpose, and
   (c) in circumstances of aggravation,
   is guilty of an offence.
   Maximum penalty: imprisonment for 5 years.

(4) In this section, *circumstances of aggravation* means circumstances in which:
   (a) the person whom the offender filmed was a child under the age of 16 years, or
   (b) the offender constructed or adapted the fabric of any building for the purpose of facilitating the commission of the offence.

Alternative verdict

(5) If on the trial of a person charged with an offence against subsection (3) the trier of fact is not satisfied that the offence is proven but is satisfied that the person has committed an offence against subsection (1), the trier of fact may acquit the person of the offence charged and find the person guilty of an offence against subsection (1). The person is liable to punishment accordingly.

Attempts

(6) A person who attempts to commit an offence under subsection (1) or (3) is liable to the penalty provided for the commission of the offence.

91L. Filming a person’s private parts

General offence

(1) A person who, for the purpose of obtaining, or enabling another person to obtain, sexual arousal or sexual gratification, films another person’s private parts, in circumstances in which a reasonable person would reasonably expect the person’s private parts could not be filmed:
   (a) without the consent of the person being filmed to being filmed for that purpose, and
   (b) knowing that the person being filmed does not consent to being filmed for that purpose,
   is guilty of an offence.
   Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

(2) An offence against subsection (1) is a summary offence.
Aggravated offence

(3) A person who, for the purpose of obtaining, or enabling another person to obtain, sexual arousal or sexual gratification, films another person’s private parts, in circumstances in which a reasonable person would expect that his or her private parts could not be filmed:

(a) without the consent of the person being filmed to being filmed for that purpose, and
(b) knowing that the person being filmed does not consent to being filmed for that purpose, and
(c) in circumstances of aggravation,

is guilty of an offence.

Maximum penalty: imprisonment for 5 years.

(4) In this section, circumstances of aggravation means circumstances in which:

(a) the person whom the offender filmed was a child under the age of 16 years, or
(b) the offender constructed or adapted the fabric of any building for the purpose of facilitating the commission of the offence.

Alternative verdict

(5) If on the trial of a person charged with an offence against subsection (3) the trier of fact is not satisfied that the offence is proven but is satisfied that the person has committed an offence against subsection (1), the trier of fact may acquit the person of the offence charged and find the person guilty of an offence against subsection (1). The person is liable to punishment accordingly.

Attempts

(6) A person who attempts to commit an offence under subsection (1) or (3) is liable to the penalty provided for the commission of the offence.

Double jeopardy

(7) A person cannot be convicted of both an offence against this section and an offence against section 91K in respect of conduct occurring on the same occasion.

91M. Installing device to facilitate observation or filming

Offence

(1) A person who, with the intention of enabling that person or any other person to commit an offence against section 91J, 91K or 91L, installs any device, or constructs or adapts the fabric of any building, for the purpose of facilitating the observation or filming of another person, is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

(2) An offence against this section is a summary offence.

Alternative verdict

(3) If on the trial of a person charged with an offence against section 91J, 91K or 91L the trier of fact is not satisfied that the offence is proven but is satisfied that the person has committed an offence against this section, the trier of fact may acquit the person of the offence charged and find the person guilty of an offence against this section. The person is liable to punishment accordingly.

Commonwealth Caribbean and Americas

CANADA

FEDERAL LEGISLATION

Criminal Code of Canada 1985 (as amended in 2005)

162. Voyeurism

(1) Every one commits an offence who, surreptitiously, observes — including by mechanical or electronic means — or makes a visual recording of a person who is in circumstances that give rise to a reasonable expectation of privacy, if

(a) the person is in a place in which a person can reasonably be expected to be nude, to expose his or her genital organs or anal region or her breasts, or to be engaged in explicit sexual activity;
(b) the person is nude, is exposing his or her genital organs or anal region or her breasts, or is engaged in explicit sexual activity, and the observation or recording is done for the purpose of observing or recording a person in such a state or engaged in such an activity; or
(c) the observation or recording is done for a sexual purpose.

Definition of visual recording
(2) In this section, visual recording includes a photographic, film or video recording made by any means.

Exemption
(3) Paragraphs (1)(a) and (b) do not apply to a peace officer who, under the authority of a warrant issued under section 487.01, is carrying out any activity referred to in those paragraphs.

Printing, publication, etc., of voyeuristic recordings
(4) Every one commits an offence who, knowing that a recording was obtained by the commission of an offence under subsection (1), prints, copies, publishes, distributes, circulates, sells, advertises or makes available the recording, or has the recording in his or her possession for the purpose of printing, copying, publishing, distributing, circulating, selling or advertising it or making it available.

Punishment
(5) Every one who commits an offence under subsection (1) or (4)
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) is guilty of an offence punishable on summary conviction.

Defence
(6) No person shall be convicted of an offence under this section if the acts that are alleged to constitute the offence serve the public good and do not extend beyond what serves the public good.

Question of law, motives
(7) For the purposes of subsection (6),
(a) it is a question of law whether an act serves the public good and whether there is evidence that the act alleged goes beyond what serves the public good, but it is a question of fact whether the act does or does not extend beyond what serves the public good; and
(b) the motives of an accused are irrelevant.

Author’s Note The recent case of R v Jarvis 2019 SCC 10 concerned a teacher who had filmed female high school students with a concealed camera, producing images focused on their faces, upper bodies and breasts. The students were unaware of the recordings. The Supreme Court of Canada held that the students had a reasonable expectation of privacy, in the sense of not being expected to be filmed in such a manner, and that the recordings were made for a sexual purpose. The Court provided the following non-exhaustive list of consideration for determining if there is a reasonable expectation of privacy:

“1) The location the person was in when she was observed or recorded. The fact that the location was one from which the person had sought to exclude all others, in which she felt confident that she was not being observed, or in which she expected to be observed only by a select group of people may inform whether there was a reasonable expectation of privacy in a particular case.
(2) The nature of the impugned conduct, that is, whether it consisted of observation or recording. Given that recording is more intrusive on privacy than mere observation, a person’s expectation regarding whether she will be observed may reasonably be different than her expectation regarding whether she will be recorded in any particular situation.
(3) Awareness of or consent to potential observation or recording.
(4) The manner in which the observation or recording was done. Relevant considerations may include whether the observation or recording was fleeting or sustained, whether it was aided or enhanced by technology and, if so, what type of technology was used.
(5) The subject matter or content of the observation or recording. Relevant considerations may include whether the observation or recording targeted a specific person or persons, what activity the person who was observed or recorded was engaged in at the relevant time, and whether the focus of the observation or recording was on intimate parts of a person’s body. This Court has recognized, in other contexts, that the nature and quality of the information at issue are relevant to assessing reasonable expectations of privacy in that information.”
162.1 Publication, etc., of an intimate image without consent

(1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty

(a) of an indictable offence and liable to imprisonment for a term of not more than five years; or

(b) of an offence punishable on summary conviction.

Definition of intimate image

(2) In this section, intimate image means a visual recording of a person made by any means including a photographic, film or video recording,

(a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;

(b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and

(c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

Defence

(3) No person shall be convicted of an offence under this section if the conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good.

Question of fact and law, motives

(4) For the purposes of subsection (3),

(a) it is a question of law whether the conduct serves the public good and whether there is evidence that the conduct alleged goes beyond what serves the public good, but it is a question of fact whether the conduct does or does not extend beyond what serves the public good; and

(b) the motives of an accused are irrelevant.

162.2 Prohibition order

(1) When an offender is convicted, or is discharged on the conditions prescribed in a probation order under section 730, of an offence referred to in subsection 162.1(1), the court that sentences or discharges the offender, in addition to any other punishment that may be imposed for that offence or any other condition prescribed in the order of discharge, may make, subject to the conditions or exemptions that the court directs, an order prohibiting the offender from using the Internet or other digital network, unless the offender does so in accordance with conditions set by the court.

Duration of prohibition

(2) The prohibition may be for any period that the court considers appropriate, including any period to which the offender is sentenced to imprisonment.

Court may vary order

(3) A court that makes an order of prohibition or, if the court is for any reason unable to act, another court of equivalent jurisdiction in the same province may, on application of the offender or the prosecutor, require the offender to appear before it at any time and, after hearing the parties, that court may vary the conditions prescribed in the order if, in the opinion of the court, the variation is desirable because of changed circumstances after the conditions were prescribed.
B. Related legislation: Voyeurism cont

Offence
(4) Every person who is bound by an order of prohibition and who does not comply with the order is guilty of
(a) an indictable offence and is liable to imprisonment for a term of not more than four years; or
(b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months.

372 False information
(1) Everyone commits an offence who, with intent to injure or alarm a person, conveys information that they know is false,
or causes such information to be conveyed by letter or any means of telecommunication.

Indecent communications
(2) Everyone commits an offence who, with intent to alarm or annoy a person, makes an indecent communication to that
person or to any other person by a means of telecommunication.

Harassing communications
(3) Everyone commits an offence who, without lawful excuse and with intent to harass a person, repeatedly communicates,
or causes repeated communications to be made, with them by a means of telecommunication.

Punishment
(4) Everyone who commits an offence under this section is
(a) guilty of an indictable offence and liable to imprisonment for a term of not more than two years; or
(b) guilty of an offence punishable on summary conviction.

Commonwealth Asia

INDIA
The Information Technology Act 2000 (as amended in 2008)
66E. Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his
or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may
extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation - For the purposes of this section-
(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;
(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) “publishes” means reproduction in the printed or electronic form and making it available for public;
(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that –
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in
a public or private place.
Commonwealth Europe

UNITED KINGDOM
ENGLAND & WALES

Sexual Offences Act 2003 (as amended by the Voyeurism (Offences) Act 2019)

67. Voyeurism

(1) A person commits an offence if-
   (a) for the purpose of obtaining sexual gratification, he observes another person doing a private act, and
   (b) he knows that the other person does not consent to being observed for his sexual gratification.

(2) A person commits an offence if-
   (a) he operates equipment with the intention of enabling another person to observe, for the purpose of obtaining sexual gratification, a third person (B) doing a private act, and
   (b) he knows that B does not consent to his operating equipment with that intention.

(3) A person commits an offence if-
   (a) he records another person (B) doing a private act,
   (b) he does so with the intention that he or a third person will, for the purpose of obtaining sexual gratification, look at an image of B doing the act, and
   (c) he knows that B does not consent to his recording the act with that intention.

(4) A person commits an offence if he instals equipment, or constructs or adapts a structure or part of a structure, with the intention of enabling himself or another person to commit an offence under subsection (1).

(5) A person guilty of an offence under this section is liable-
   (a) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both;
   (b) on conviction on indictment, to imprisonment for a term not exceeding 2 years.

67A Voyeurism: additional offences

(1) A person (A) commits an offence if-
   (a) A operates equipment beneath the clothing of another person (B),
   (b) A does so with the intention of enabling A or another person (C), for a purpose mentioned in subsection (3), to observe-
      (i) B’s genitals or buttocks (whether exposed or covered with underwear), or
      (ii) the underwear covering B’s genitals or buttocks, in circumstances where the genitals, buttocks or underwear would not otherwise be visible, and
   (c) A does so-
      (i) without B’s consent, and
      (ii) without reasonably believing that B consents.

(2) A person (A) commits an offence if-
   (a) A records an image beneath the clothing of another person (B),
   (b) the image is of-
      (i) B’s genitals or buttocks (whether exposed or covered with underwear), or
      (ii) the underwear covering B’s genitals or buttocks, in circumstances where the genitals, buttocks or underwear would not otherwise be visible, B
   (c) A does so with the intention that A or another person (C) will look at the image for a purpose mentioned in subsection (3), and
   (d) A does so-
      (i) without B’s consent, and
      (ii) without reasonably believing that B consents.
(3) The purposes referred to in subsections (1) and (2) are—
   (a) obtaining sexual gratification (whether for A or C);
   (b) humiliating, alarming or distressing B.

(4) A person guilty of an offence under this section is liable—
   (a) on summary conviction, to imprisonment for a term not exceeding 12 months, or to a fine, or to both;
   (b) on conviction on indictment, to imprisonment for a term not exceeding 2 years.

68. Voyeurism: interpretation

(1) For the purposes of section 67, a person is doing a private act if the person is in a place which, in the circumstances, would reasonably be expected to provide privacy, and—
   (a) the person’s genitals, buttocks or breasts are exposed or covered only with underwear,
   (b) the person is using a lavatory, or
   (c) the person is doing a sexual act that is not of a kind ordinarily done in public.

(1A) For the purposes of sections 67 and 67A, operating equipment includes enabling or securing its activation by another person without that person’s knowledge.

(2) In section 67, “structure” includes a tent, vehicle or vessel or other temporary or movable structure.
C. Jurisdiction

Commonwealth Africa

BOTSWANA

Cybercrime and Computer Related Crimes Act 2018

3. Jurisdiction

The courts of Botswana shall have jurisdiction where an act done or an omission made constituting an offence under this Act has been committed

(a) in the territory of Botswana;

(b) by a national of Botswana outside the territory of Botswana, if the person's conduct would also constitute an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country;

(c) on a ship or aircraft registered in Botswana;

(d) in part in Botswana; or

(e) outside the territory of Botswana and where any result of the offence has an effect in Botswana.

33. Extradition

An offence under this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

NAMIBIA

Cybercrimes Bill 2019 (not yet in force)

17. Extra-territorial effect

For all purposes in law, an offence in terms of this Act is deemed to have been committed in Namibia, if -

(a) any act of preparation towards the offence or any part of the offence was performed in Namibia;

(b) the offence was committed on a ship or aircraft registered in Namibia;

(c) the offence was committed by a citizen of Namibia; or

(d) an information system in Namibia was affected by the offence or any person in Namibia suffered loss, damage to property or any other disadvantage or infringement of his or her rights as a result of the offence.

...
74. Co-operation with foreign authorities

(1) The Inspector-General of the Namibian Police may agree with any institution or body of another country to co-operate in the investigation or prosecution of an offence under this Act or another offence whose investigation reasonably requires the performance of an action referred to in paragraph (a) or (b) of subsection (2).

(2) If an agreement has been concluded under subsection (1) -

(a) any power of investigation provided for in this Act or the Criminal Procedure Act, 1977 (Act No. 51 of 1977) may be exercised in respect of an offence covered by the agreement as if that offence were committed in Namibia;

(b) information stored in terms of section 71(2) and obtained in terms of section 73 of the Communications Act may be provided to the institution or body as if the offence were committed in Namibia;

(c) any information obtained by an investigation in Namibia may be communicated to the institution or authority in question;

(d) any information obtained from the institution or authority in question, may be used in any investigation in Namibia,

and a document purporting to be an affidavit or similar declaration by a person in the country concerned may be used as supporting information to obtain a warrant or authorisation under this Act or the Criminal Procedure Act, 1977 (Act No. 51 of 1977) or regulations made under ??; and

(e) despite any requirement in the law of Namibia for the authentication of documents created outside Namibia, a document created as a result of an investigation under that agreement may be used in criminal proceedings as if that document have been created inside Namibia.

(3) If a request has been made in terms of section 7 of the International Co-operation in Criminal Matters Act, 2000 Act No. 9 of 2000 the provisions of subsection (2) apply in respect of anything done as a result of such request.

SOUTH AFRICA

Cybercrimes Bill 2017 [not yet in force]

23. Jurisdiction

(1) A court in the Republic trying an offence has jurisdiction where -

(a) an offence in terms of Part I or Part II of Chapter 2 was committed-

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed;

(b) an offence in terms of Part I or Part II of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is citizen of the Republic or ordinarily resident in the Republic;

(c) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is-

(i) a company, incorporated or registered as such under any law, in the Republic; or

(ii) any body of persons, corporate or unincorporated, in the Republic;

(d) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against -

(i) a restricted computer system contemplated in section 11(1)(b); or

(ii) a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or

(e) any act in preparation of an offence in terms of Part I or Part II of Chapter 2, or any action necessary to commit the offence took place -

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed.
(2) If the act alleged to constitute an offence in terms of Part I or Part II of Chapter 2 was committed outside the Republic, a court of the Republic, regardless of whether or not the act constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged -
   (a) is a citizen of the Republic or ordinarily resident in the Republic;
   (b) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;
   (c) is a company, incorporated or registered as such under any law, in the Republic; or
   (d) any body of persons, corporate or unincorporated, in the Republic.

(3) Any act alleged to constitute an offence in terms of Part I or Part II of Chapter 2 and which was committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act constitutes an offence or not at the place of its commission, deemed also to have been committed in the Republic if that-
   (a) person is found to be in South Africa; and
   (b) person is for one or other reason not extradited to, or by South Africa, or if there is no application to extradite that person.

(4) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted.

(5) (a) A prosecution in terms of subsections (2) and (3) -
   (i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and
   (ii) must commence before a court designated by the National Director of Public Prosecutions.

(b) A copy of the written permission and designation must be served on the accused and the original thereof must be handed in at the court in which the proceedings are to commence.

(6) The National Commissioner and the National Head of the Directorate, respectively, in consultation with the National Director of Public Prosecutions must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act regarding the investigation of offences that was committed outside the Republic.

TANZANIA

Cybercrime Act 2015

30. Jurisdiction

(1) The courts shall have jurisdiction to try any offence under this Act where an act or omission constituting an offence is committed wholly or in part -
   (a) within the United Republic of Tanzania;
   (b) on a ship or aircraft registered in the United Republic of Tanzania;
   (c) by a national of the United Republic of Tanzania;
   (d) by a national of the United Republic of Tanzania who resides outside the United Republic of Tanzania, if the act or omission would equally constitute an offence under a law of that country; or
   (e) by any person, irrespective of his nationality or citizenship, or location, when the offence is:
      (i) committed using a computer system, device or data located within United Republic of Tanzania; or
      (ii) directed against computer system, device or data or person located in United Republic of Tanzania.

(2) In this section the term “court” means court of competent jurisdiction.
C. Jurisdiction cont

UGANDA

Computer Misuse Act 2011

30. Territorial jurisdiction

(1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

(3) For the purposes of this Act, this section applies if, for the offence in question-
   (a) the accused was in Uganda at the material time; or
   (b) the computer, program or data was in Uganda at the material time.

ZIMBABWE

Cybercrime and Cybersecurity Bill 2017 (draft – not in force yet)

38. Jurisdiction

(1) A court in Zimbabwe shall have jurisdiction to try any offence under this Act where the offence was committed wholly or in part-
   (a) within Zimbabwe or by any person in or outside Zimbabwe using a computer or information system or device, software or data located in Zimbabwe; or
   (b) on a ship or aircraft registered in Zimbabwe; or
   (c) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe, whether or not the offence is committed in Zimbabwe; or
   (d) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside Zimbabwe, if the person’s conduct also constitutes an offence under the law of the country where the offence was committed and harmful effects were caused in Zimbabwe; or
   (e) by any person, regardless of the location, nationality or citizenship of the person
      (i) using a computer or information system or device, software, or data located within Zimbabwe; or
      (ii) directed against a computer or information system or device, software or data located in Zimbabwe.

39. Extradition

Any offence in terms of this Act shall be subject to extradition in terms of the Extradition Act [Chapter 9:08] provided that a person may not be extradited to or from Zimbabwe unless his or her conduct is criminal in both Zimbabwe and the other country.
17. Application to person outside Singapore

(1) Without prejudice to the jurisdiction and power conferred under this Act or any other written law, the court shall in the circumstances specified in subsections (2) to (6) -
   (a) have jurisdiction to try any offence under section 3, 4, 5, 6 or 7 and impose the full punishment under this Act; and
   (b) have jurisdiction to make any order under section 12 or 13 on the basis of a contravention of section 3, 4, 5, 6 or 7.

(2) Where the victim under section 3, 4, 5 or 6 was outside Singapore when the accused or respondent (as the case may be) used the words or behaviour, made the communication or published the identity information, in contravention of any such section, the court shall have jurisdiction if the accused or respondent (as the case may be) was in Singapore when the accused or respondent used those words or behaviour or made that communication or published that identity information, as the case may be.

(3) Where the accused or respondent (as the case may be) was outside Singapore when that accused or respondent used the words or behaviour, or made the communication or published the identity information, in contravention of section 3, the court shall have jurisdiction if -
   (a) the victim of the contravention was in Singapore when the use of those words or behaviour, or the making of that communication or that publication of identity information, caused the victim harassment, alarm or distress; and
   (b) the accused or respondent (as the case may be) knew or had reason to believe that the victim of the contravention would be in Singapore at the time referred to in paragraph (a).

(4) Where the accused or respondent (as the case may be) was outside Singapore when that accused or respondent used the words or behaviour, or made the communication or published the identity information, in contravention of section 4, 5 or 6, the court shall have jurisdiction if -
   (a) the victim of the contravention was in Singapore when the victim heard, saw or otherwise perceived those words or behaviour or that communication or that identity information; and
   (b) the accused or respondent (as the case may be) knew or had reason to believe that the victim of the contravention would be in Singapore at the time referred to in paragraph (a).

(5) Where the victim under section 7 was outside Singapore when any of the acts or omissions associated with unlawful stalking occurred in contravention of that section, the court shall have jurisdiction if the accused or respondent (as the case may be) was in Singapore when any of those acts or omissions occurred.

(6) Where the accused or respondent (as the case may be) was outside Singapore when any of the acts or omissions associated with unlawful stalking occurred in contravention of section 7, the court shall have jurisdiction if -
   (a) the victim of the contravention was in Singapore when any of those acts or omissions occurred; and
   (b) the accused or respondent (as the case may be) knew or had reason to believe that the victim of the contravention was in Singapore at the time referred to in paragraph (a).

(7) Without prejudice to the jurisdiction and power conferred under this Act or any other written law, the court shall in the circumstances specified in subsections (8) and (9) have jurisdiction to try any offence under section 10 for failure to comply with an order and impose the full punishment under this Act.

(8) In the case of an order prohibiting the respondent from doing any thing in relation to the victim or to any related person specified in the order, where the victim or the related person was outside Singapore when the respondent did any thing prohibited by the order, the court shall have jurisdiction if the respondent was in Singapore when that respondent did that thing.
C. Jurisdiction cont

(9) In the case of an order prohibiting the respondent from doing any thing in relation to the victim or to any related person specified in the order, the court shall have jurisdiction -
(a) where the respondent was outside Singapore when that respondent failed to comply with an order prohibiting him from doing any thing in relation to the victim, if -
   (i) the victim was in Singapore when the thing done by the respondent in contravention of the order was heard, seen or otherwise perceived by the victim; and
   (ii) the respondent knew or had reason to believe that the victim would be in Singapore at the time referred to in sub-paragraph (i);
(b) where the respondent was outside Singapore when that respondent failed to comply with an order prohibiting him from doing any thing in relation to any related person specified in the order (in the case of a contravention of section 7), if -
   (i) the related person was in Singapore when the thing done by the respondent in contravention of the order was heard, seen or otherwise perceived by the related person; and
   (ii) the respondent knew or had reason to believe that the related person would be in Singapore at the time referred to in sub-paragraph (i); and
(c) where the respondent was outside Singapore when that respondent failed to comply with an order prohibiting him from publishing or continuing to publish any communication, if -
   (i) the communication was heard, seen or otherwise perceived by a section of the public in Singapore; and
   (ii) the respondent knew or had reason to believe that communication would be heard, seen or otherwise perceived by a section of the public in Singapore.

(10) In subsections (8) and (9) -
(a) “victim”, in relation to an offence under section 10 for failure to comply with an order, means the victim under section 3, 4, 5, 6 or 7, as the case may be, in whose favour the order was made;
(b) “respondent”, in relation to an offence under section 10 for failure to comply with an order, means the person who is alleged to have failed to comply with the order in contravention of section 10; and
(c) a reference to any thing done by the respondent includes any words or behaviour used or communication made by the respondent.

International & Regional Conventions

Council of Europe Convention on Cybercrime 2001 (Budapest Convention)

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a) in its territory; or
   b) on board a ship flying the flag of that Party; or
   c) on board an aircraft registered under the laws of that Party; or
   d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
**Article 24 – Extradition**

1. (a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

   (b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7. (a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

   (b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

**Article 25 – General principles relating to mutual assistance**

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.
Council of Europe Protection of Children against Sexual Exploitation and Sexual Abuse Convention 2007 (Lanzarote Convention)

Article 25 – Jurisdiction

1. Each Party shall take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention, when the offence is committed:
   a) in its territory; or
   b) on board a ship flying the flag of that Party; or
   c) on board an aircraft registered under the laws of that Party; or
   d) by one of its nationals; or
   e) by a person who has his or her habitual residence in its territory.

2. Each Party shall endeavour to take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention where the offence is committed against one of its nationals or a person who has his or her habitual residence in its territory.

3. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraph 1.e of this article.

Convention on preventing and combating violence against women and domestic violence 2011 (Istanbul Convention)

Article 44 – Jurisdiction

(1) Parties shall take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention, when the offence is committed:
   a) in their territory; or
   b) on board a ship flying their flag; or
   c) on board an aircraft registered under their laws; or
   d) by one of their nationals; or
   e) by a person who has her or his habitual residence in their territory.

(2) Parties shall endeavour to take the necessary legislative or other measures to establish jurisdiction over any offence established in accordance with this Convention where the offence is committed against one of their nationals or a person who has her or his habitual residence in their territory.

(3) For the prosecution of the offences established in accordance with Articles 36, 37, 38 and 39 of this Convention, Parties shall take the necessary legislative or other measures to ensure that their jurisdiction is not subordinated to the condition that the acts are criminalised in the territory where they were committed.

(4) For the prosecution of the offences established in accordance with Articles 36, 37, 38 and 39 of this Convention, Parties shall take the necessary legislative or other measures to ensure that their jurisdiction as regards points d and e of paragraph 1 is not subordinated to the condition that the prosecution can only be initiated following the reporting by the victim of the offence or the laying of information by the State of the place where the offence was committed.

(5) Parties shall take the necessary legislative or other measures to establish jurisdiction over the offences established in accordance with this Convention, in cases where an alleged perpetrator is present on their territory and they do not extradite her or him to another Party, solely on the basis of her or his nationality.

(6) When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult each other with a view to determining the most appropriate jurisdiction for prosecution.

(7) Without prejudice to the general rules of international law, this Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its internal law.

Article 17 Jurisdiction and coordination of prosecution

1. Member States shall take the necessary measures to establish their jurisdiction over the offences referred to in Articles 3 to 7 where:
   (a) the offence is committed in whole or in part within their territory; or
   (b) the offender is one of their nationals.

2. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 7 committed outside its territory, inter alia, where:
   (a) the offence is committed against one of its nationals or a person who is an habitual resident in its territory;
   (b) the offence is committed for the benefit of a legal person established in its territory; or
   (c) the offender is an habitual resident in its territory.

3. Member States shall ensure that their jurisdiction includes situations where an offence referred to in Articles 5 and 6, and in so far as is relevant, in Articles 3 and 7, is committed by means of information and communication technology accessed from their territory, whether or not it is based on their territory.

4. For the prosecution of any of the offences referred to in Article 3(4), (5) and (6), Article 4(2), (3), (5), (6) and (7) and Article 5(6) committed outside the territory of the Member State concerned, as regards paragraph 1(b) of this Article, each Member State shall take the necessary measures to ensure that its jurisdiction is not subordinated to the condition that the acts are a criminal offence at the place where they were performed.

5. For the prosecution of any of the offences referred to in Articles 3 to 7 committed outside the territory of the Member State concerned, as regards paragraph 1(b) of this Article, each Member State shall take the necessary measures to ensure that its jurisdiction is not subordinated to the condition that the prosecution can only be initiated following a report made by the victim in the place where the offence was committed, or a denunciation from the State of the place where the offence was committed.

SADC Protocol on Mutual Legal Assistance in Criminal Matters 2002

Article 2 Scope of Application and Obligation to Provide Mutual Legal Assistance

1. The State Parties shall, in accordance with this Protocol, provide each other with the widest possible measure of mutual legal assistance in criminal matters.

2. Mutual legal assistance is any assistance given by the Requested State in respect of investigations, prosecutions or proceedings in the Requesting State in a criminal matter, irrespective of whether the assistance is sought or is to be provided by a court or some other competent authority.

3. Criminal matters include investigations, prosecutions or proceedings relating to offences concerning transnational organized crime, corruption, taxation, custom duties and foreign exchange control.

4. Assistance shall be provided without regard to whether the conduct which is the subject of investigation, prosecution, or proceedings in the Requesting State would constitute an offence under the laws of the Requested State.

SADC Model Law on Computer Crime and Cybercrime 2013

23. Jurisdiction

This Act applies to an act done (offence committed) or an omission made:

(a) in the territory of [enacting country]; or

(b) on a ship or aircraft registered in [enacting country]; or

(c) by a national of [enacting country] outside the jurisdiction of any country; or

(d) by a national of [enacting country] outside the territory of [enacting country], if the person’s conduct would also constitute an offence under a law of the country where the offence was committed.