Commonwealth Cybercrime Monitor

March 2023

The Commonwealth

Commonwealth Cybercrime Monitor

The Commonwealth

Foreign, Commonwealth
& Development Office

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

List of Cases

AFRICA

ESWATINI

THE GAMBIA

GHANA

KENYA

MAURITIUS

NAMIBIA

NIGERIA

RWANDA

SEYCHELLES

SOUTH AFRICA

UGANDA

TANZANIA

ASIA

BRUNEI DARUSSALAM

INDIA

MALAYSIA

SINGAPORE

CARIBBEAN AND AMERICAS

THE BAHAMAS

BELIZE

CANADA

JAMAICA

SAINT LUCIA

TRINIDAD AND TOBAGO

EUROPE

CYPRUS

MALTA

UNITED KINGDOM

PACIFIC

AUSTRALIA

FIJI

NEW ZEALAND

PAPUA NEW GUINEA

SAMOA

TONGA

VANUATU

Preface

The *Commonwealth Cybercrime Monitor* (CCM) contains a brief synopsis and links to selected cybercrime cases collected from different countries across the Commonwealth. It will be of interest to policymakers, academics and practitioners involved in cybercrime policymaking, investigation, prosecution and adjudication. It is designed to assist Commonwealth member countries to strengthen their anti-cybercrime and cybersecurity legislative, policy, institutional and multilateral frameworks.

The cases covered in the present edition of the CCM include online harassment, ransomware, child pornography, money laundering and electronic fraud cases.

The Commonwealth Secretariat is grateful to the UK Foreign, Commonwealth & Development Office (FCDO), which provided funding for this publication under its Commonwealth Cyber Capability Programme to further the implementation of the Commonwealth Cyber Declaration that was endorsed by Commonwealth Heads of State in 2018.

The Commonwealth Secretariat Cyber Unit has also produced a Wiki, which provides an overview of the national cybersecurity strategic plans, cybercrime and cybersecurity laws of each Commonwealth member country. The Wiki will be updated at regular intervals.

Please note that there is some explicit language included in this publication which has been taken from one of the cases discussed.

Acknowledgments

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development (UK FCDO) to the Commonwealth Cyber Capability Programme.

The Commonwealth Cybercrime Monitor (CCM) cases were researched, collated and analysed by Ms Georgia Brown and Ms Amani Ukaegbu under the general guidance of Dr Tawanda Hondora, Adviser and Head of Rule of Law Section Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer - Cyber Capability Programme (GPD), led and co-ordinated the review and editorial process of the CCM. Ms Emma Beckles, Programme Officer - GPD and Mr. Shakirudeen Ade Alade, Programme Coordinator - GPD provided valuable input while Ms Helene Massaka, Programme Assistant - GPD, provided logistical and administrative support.

The team is grateful for the constructive feedback received from internal reviewers Mr Clive Lawson, Publications Assistant - Communication Division, Ms Madonna Akabuno and Ms Nyla Thomas, our work experience students, for their assistance in producing the CCM.

Acronyms and Abbreviations

ACA	Anti-Corruption Act 2009 (Uganda)
A$	Australian dollars
CA	Cybercrime Act 2015 (Nigeria)
CCA	Computer Crimes Act 1997 (Malaysia)
CJCA	Criminal Justice and Courts Act 2015 (United Kingdom)
CMA	Computer Misuse Act 2011 (Uganda), Computer Misuse Act 1990 (United Kingdom)
CMCA	Computer Misuse and Cybercrime Act 2018 (Kenya)
CPS	Calgary Police Service
C$	Canadian dollar
DPP	Director of Public Prosecutions (Kenya, Australia)
EFF	Economic Freedom Fighters (South Africa)
FA	Fraud Act 2006 (UK)
GDF	Guyana Defence Force
GDPR	General Data Protection Regulation (European Union)
GPF	Guyana Police Force
G$	Guyana dollar
HDCA	Harmful Digital Communications Act 2015 (New Zealand)
IP	internet protocol (address)
ICA	Information and Communications (Amendment) Act 2013 (The Gambia)
ICO	Information Commissioners Office (UK)
ICTA	Information and Communication Technologies Act 2001 (Mauritius)
IT	information technology
J$	Jamaican dollar
N	naira
N$	Namibia dollar
PC	Penal Code (The Bahamas)
PCA	Proceeds of Crime Act 2002 (UK)
PDPA	Personal Data Protection Act 2012 (Singapore)
RF	Rwanda franc
RM	ringgit (Malaysia)

SCA	Serious Crime Act 2007 (UK)
SOCU	Special Organised Crime Unit (Guyana)
TSh	Tanzanian shilling
TT$	Trinidad and Tobago dollar
URA	Uganda Revenue Authority
USh	Uganda shilling
V	victim
Vt	vatu

CASE ANALYSES – AFRICA

ESWATINI

Title: *Exalto v Royal Eswatini National Airways and Another* (2258 of 2020) [2022] SZHC 40 (25 March 2022)

Weblink: Judgment

Issue: Whether publishing comments about an employer on social media was protected by the constitutional right to freedom of speech.

Legislation

- The Constitution

Facts

The applicant's employer instituted disciplinary proceedings against the applicant, alleging that he had brought disrepute against the employer through the use of social media – by publishing a post on his Facebook page.

The applicant brought these proceedings to the High Court, inviting the court to interdict the disciplinary proceedings and seeking a declaratory order to the effect that he was exercising his constitutional rights to freedom of speech and opinion under Section 23 and 24 of the Constitution.

Decision of the court

The respondent failed in opposing the application for declaratory relief.

The High Court held:

(i) That it did have jurisdiction to deal with the matter.

(ii) That the case required assessment of the merits to determine whether reference to constitutional provisions were applicable (that is, whether the doctrine of avoidance was applicable in the alternative). The Industrial Court is not competent to do so, even cursorily.

(iii) Even if the court adopted the doctrine of avoidance, the constitutional issue was bound to arise again in the Industrial Court, or before the disciplinary chairperson, as the applicant canvassed his defence.

(iv) The applicant's Facebook page was within the constitutional provisions of section 23(1)(2) and section 24(1)(2).

(v) The clawback clauses of section 23(2) and section 24(2)(3) allowed hindrance on the exercise of those rights in exceptional circumstances. The facts in this case fell outside the exceptional circumstances recognised by the Constitution, hence the post was in exercise of the applicant's constitutional rights.

(vi) The rights in section 14, 23 and 24 of the Constitution were not derogable except to the extent that the Constitution expressly provides.

Title: *Shongwe v The Swazi Observer (Pty)* (847 of 2015) [2021] SZHC 212 (11 November 2021)

Weblink: Judgment

Issue: Defamation.

Cases cited

- *National Media Ltd and others v Bogoshi* 1998
- *Mountain Oaks Winery (Pty) Ltd and another v Marrion Smith and another*
- *Khumalo and others v Holomisa* (CCT 53/01) [2002] ZACC; 2002 (5) SA 401
- *Olomisa v Argus Newspapers Ltd* 1996 (2) SA 588

Facts

The claimant launched a defamation suit against the defendant, a national newspaper, for the publication of defamatory material about him on the defendant's website. The claimant contended that the contents of the article were untrue, fabricated, wrongful and grossly defamatory as they conveyed the message to ordinary readers of the defendant's newspaper that he was a fraudster and/or thief, and not trustworthy with finances. A week later the newspaper published a retraction and apology for the alleged defamatory publication, after discovering the claims were false and defamatory to the claimant. The

claimant argued that prior to the publication, he enjoyed a good and untainted reputation among the citizens of Eswatini and was regarded as a respectable and noble family man.

Decision of the court

Dismissing the claim, the court held that the timeous apology and retraction of the original story by the defendant was carried out in a manner that was exhibited with reasonable conduct and lack of negligence on the part of the defendant. It also found that the comments were not reported as a factual statement, but rather as allegations which were being probed. Given that the defendant had transparently and bona fide admitted its fault, apologised and retracted the material, this indicated a lack of intention to injure the claimant.

THE GAMBIA

Title: *Touray & 2 others v The Attorney General, SC Civil Suit N0. 001/2017* (9 May 2018)

Weblink: Judgment

Issue: Defamation.

Legislation

- Sections 178, 179, 180, 181A of the Criminal Code
- Section 173A(1)(a) and (c) of the Information and Communications (Amendment) Act 2013
- Section 25 of the Constitution

Facts

The plaintiffs brought an application before the Supreme Court of The Gambia, arguing that the provisions in the Criminal Code relating to the offences of criminal defamation, libel and false news online were unconstitutional. These provisions, inter alia, made it a criminal offence to 'a. spread false news against the government or public officials; b. caricature, abuse or make derogatory statements against the person or character of officials'.

The key issues before the court were:

(a) whether sections 178, 179, 180 and 181A of the Criminal Code met the test for restriction under section 25(4) and section 209 of the Constitution and therefore be considered valid; and

(b) whether section 173A(1)(a) and (c) of the Information and Communications (Amendment) Act (ICA) 2013 was consistent with section 25(1)(a) and (b) of the Constitution and if the sanction applicable to a conviction under the section of the Act was justified and proportionate.

The plaintiffs submitted that the definitions of 'libel', 'defamatory matter' and 'publication', and provision for criminal offences committed over the internet were too vague and thus risked being abused by those seeking to enforce them for a purpose other than the legitimate aim of the legislation. The plaintiffs further argued that the provisions placed unjustified limitations on freedom of speech, as it was unclear what remarks would attract prosecution. They argued that this did not meet the requirement of section 25(4) of the Constitution, which demands any limitation must be 'necessary in a democratic society'.

Another issue raised by the plaintiffs was that the legislation imposed strict criminal liability, allowing prosecution even for unintentional publication of incorrect information with stiff penalty. This precludes traditional defences for defamation such as justification, truth, qualified privilege and fair comment.

Decision of the court

The Supreme Court first dealt with whether the challenge to section 173 of the ICA 2013 could be pleaded, despite not being specifically prayed for in the Writ of Summons. It held as an exception and not precedent, it could, due to the importance of the matter and in the interest of justice.

Considering the constitutionality of the provisions, the court referred to its judgement of *Gambia Press Union and 2 Ors v The Attorney General* [2018] delivered on 9 May 2018. In that case section 181A of the Criminal Code was upheld as constitutional. The court saw no reason to depart from that finding.

The Supreme Court noted there was a presumption of constitutionality, and the burden of proof to challenge any provision in this regard lay with the plaintiff. It considered any limitation on fundamental rights was only lawful if three conditions were satisfied: (i) reasonable; (ii) necessary in a democratic society; and (iii) imposed for one or more of the purposes set out in sections 25(4)

and 209 of the Constitution, i.e. 'necessary in a democratic society and required in the interests of the sovereignty and integrity of The Gambia, national security, public order, decency or morality, or in relation to contempt of court' [32], and 'reasonably required in a democratic society in the interest of national security, public order, public morality and for the purpose of protecting the reputations, rights and freedoms of others' [36].

The court held that sections 178, 179, 180 of the Criminal Code were inconsistent with the constitutional guarantees of freedom of speech and freedom of the press. It found that the limitations were neither reasonable nor necessary in a democratic society and the provisions failed to demonstrate a legitimate aim as required by the Constitution. The court noted that the original provisions, although since amended, pre-dated the current Constitution and took 'what some may describe as a colonial-era approach to protecting citizens' [28]. It considered that the provisions at this time, in the current constitutional context, did not continue to serve a purpose that accords with the current Constitution.

For the same reasons, the court found that section 173A(1)(a) and (c) of the Information and Communications (Amendment) Act 2013 was also inconsistent with the rights enshrined in the Constitution, and that the penalty was disproportionate. The court thus declared sections 178, 179, 180 of the Criminal Code and 173A(1)(a) and (c) of the Information and Communications (Amendment) Act 2013 ultra vires the Constitution and therefore invalid.

GHANA

Title: *Republic v High Court (General Jurisdiction) Accra; Ex-parte Dr Rawlings* (J5 19 of 2016) [2016] GHASC 18 (19 May 2016)

Weblink: Judgment

Issue: Money laundering.

Legislation

- Section 23(1) and 131(1) of the Criminal Offences Act 1960 (Act 29)
- Section 123 of the Electronic Transactions Act 2008 (Act 772)
- Section 1(1) of the Anti-Money Laundering (Amendment) Act 2014 (Act 874)

Facts

The complainant was a citizen/resident of Australia. The three accused persons were Ghanaians. In December 2011, the complainant was contacted by a person on a dating website in 2011 who introduced himself as 'Steve Gauman', a German citizen with Australian residence (the second accused). They communicated via email. The second accused asked the complainant to meet him in Perth, but later cancelled the meeting saying he had to travel overseas for work. The complainant received a telephone call from the second accused, telling her that he was in Ghana staying at a hotel, but his Australian bank accounts had been frozen due to tampering in the past and he only had bank cheques with him. The second accused pleaded with the complainant, and she sent A$2,000 Australian dollars (A$) through Western Union because she felt sorry for him. She sent a further A$169,597.82 for an 'supposedly unforeseen plight' the accused was in.

The second accused later introduced the first accused to the complainant as a person employed by a shipping company in Accra and as the person assigned to assist the second accused in unloading his shipping containers. The first accused told the complainant that he had been detained in the United Kingdom (UK) by customs for carrying gold in his bags taken from Accra without authorised documentation. The second accused requested the complainant to send money to the first accused via bank transfer, whereby he received A$211,346.53. When the merchant bank account froze the account of the first accused, the second accused tried to convince the complainant to write to the bank and send more money, which she declined to do.

The second accused then introduced the third accused as a close friend to receive funds on his behalf through money transfers and bank accounts. The third accused, with the first and second accused, assumed different names to defraud the complainant of A$67,082.83 through bank account and international money transfers.

The three defendants were subject to investigations which revealed that from 2011 to 2014, they had defrauded the claimant through the internet of A$448,027. Charges were brought for conspiracy to defraud contrary to section 23(1) and 131(1) of the Criminal Offences Act 1960 (Act 29) and section 123 of the Electronic Transactions Act

2008 (Act 772), defrauding under false pretences contrary to section 131(1) of Act 29 and section 123 of Act 772, and money laundering contrary to section 1(1) of the Anti-Money Laundering (Amendment) Act 2014 (Act 874).

Decision of the court

On the charge of conspiracy to commit crime (defrauding by false pretences), the court found the first and second defendants guilty. They had made false pretences about who they were, their location, and lied about the reasons the money was needed. The bank account of the first defendant was used as a conduit for some of the funds and the second defendant had created a false identity to communicate with complainant. It was therefore clear that a substantial amount of money was parted with by the complainant who parted with the money upon false/fraudulent representations made to her. The court noted that although there were errors with the data supplied, it would be disingenuous for anyone to argue that 'Steve Gauman' should be produced when he was created by the false profile of the second defendant. On counts three and five (money laundering), it was apparent from the evidence that the monies were all proceeds of the crime of defrauding by false pretences and all three accused were convicted on counts three and five for offending against the Anti-Money Laundering (Amendment) Act 2014.

All three defendants were imprisoned for 4 years on each count and ordered to pay 20,000 new cedi (¢) and US$10,000 within 21 days to the complainant.

KENYA

Title: *Patroba Michieka Omwenga v Republic [2022]* EKLR (Miscellaneous Criminal Application E150 of 2021); (28 February 2022) (High Court)

Weblink: Judgment

Issue: Application to the High Court to transfer a trial for alleged cyber harassment and publishing false information from Voi Chief Magistrate's Court to Milimani Nairobi Magistrate's Court.

Legislation

- Section 27 and 23 of the Computer Misuse and Cybercrime Act of 2018
- Section 72 of the Criminal Procedure Code

Facts

The defendant sent an offensive message to the victim via WhatsApp and published a statement on his Facebook page that was 'false and calculated to discredit the reputation' of the victim and his law firm [3]. The defendant was charged with cyber harassment, contrary to section 27 of the Computer Misuse and Cybercrime Act (CMCA) of 2018, and publication of false information, contrary to section 23 of the CMCA 2018.

The defendant made an urgent application to the High Court to transfer the case from Voi Chief Magistrate's Court to Milimani Nairobi Magistrate's Court. The applicant submitted, *inter alia*, that the offence took place in Nairobi and should therefore be tried there under section 72 of the Criminal Procedure Code.

Decision of the court

The court noted that the charge sheet indicates the offence was conducted at an 'unknown place'. The court further noted that as the offence was allegedly committed through a digital platform, the location of the device when the offensive message was sent could be found upon analysing the gadget or other telephone service providers' sources of information [18].

The court allowed the application and made an order to transfer the case.

Title: *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others;* Article 19 East Africa & another (Interested Parties); Constitutional Petition No. 206 of 2019, [2020] eKLR

Weblink: Judgment

Issue: The petitioners alleged various provisions of the Computer Misuse and Cybercrime Act 2018 were unconstitutional.

Legislation

- Section 2 of the Computer Misuse and Cybercrime Act 2018; false publication
- Section 23 of the Computer Misuse and Cybercrime Act 2018; publication of false information
- Section 24 of the Computer Misuse and Cybercrime Act 2018; child pornography

- Section 27 of the Computer Misuse and Cybercrime Act 2018; cyber harassment
- Section 28 of the Computer Misuse and Cybercrime Act 2018; cybersquatting
- Section 37 of the Computer Misuse and Cybercrime Act 2018; wrongful distribution of obscene or intimate images

Facts

The Computer Misuse and Cybercrime Act 2018 (hereinafter referred to as the 'CMCA 2018') was assented to law on 16 May 2018, having been considered and passed by the National Assembly. It is an Act of parliament to provide for offences relating to computer systems; to enable timely and effective detection; prohibition, prevention, response; investigation and prosecution of computer and cybercrimes to facilitate international co-operation in dealing with computer and cybercrimes matters, and for connected purposes.

The petitioners challenged the constitutional validity of the above sections on the grounds that requirement of public participation was not satisfactorily met during the consideration of the Bill and further that the sections violated the provisions of Article 24 of the Constitution on limitation of rights and fundamental freedoms. It was further argued that section 23 of the CMCA 2018 was similar to section 29 of the Kenya Information and Communication Act, which was declared unconstitutional in *Geoffrey Andere v Attorney General & 2 others* [2016] eKLR. It was therefore argued that section 23 also reintroduced criminal defamation, formerly based on section 194 of the Penal Code, which was declared unconstitutional in *Jackueline Okuta & another v Attorney General & 2 others* [2017] eKLR. Finally, the petitioners submitted that section 24 of the CMCA 2018 was unclear, asking whether removal of the word 'child' before pornography in section 24(1)(c) of the Act was intentional, as section 24 is titled to deal with child pornography. It was asserted that forbidding the consumption and production of pornography as set out under section 24(1)(c) of the Act therefore limited the right to freedom of expression.

Decision of the court

The High Court (Makau J) delineated eight issues for determination. Pertinent to this summary are three issues, namely:

- whether sections 22, 23, 23, 24(1)(c), 27, 28 and 37 of the Act limit Articles 32, 33 and 34 of the Constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010;
- whether sections 16, 17, 31, 32, 34, 35, 36, 38(1), 38(2), 39 and 41 of the Act are inconsistent with the Constitution by failing to prescribe the mens rea element of the offence they create; and
- whether section 48, 50, 51, 52 and 53 of the Act limit Article 31 of the Constitution in a manner inconsistent with Article 24 of the Constitution of Kenya 2010.

In a judgment delivered on 20 February 2020, the court held that the Computer Misuse and Cybercrimes Act 2018 was valid and did not violate, infringe or threaten fundamental rights and freedoms and was justified under Article 24 of the Constitution and that Sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52, and 53 of the Computer Misuse and Cybercrimes Act were constitutional and did not violate, infringe and/or threaten fundamental rights and freedoms.

The court reasoned that the imminent danger lay in the inability of the law enforcers to ensure national security in view of the cybercrimes and computer misuse offences. Consequently, it found that the need to protect the wider public from the dangers in the cyberspace outweighed the granting of the petition. Upon examination of the impugned provisions of the Act, the learned judge found that the same effectively protected the public interest and as such the public interest needed to be held in the highest esteem.

Title: *Wesley Ngerechi & another v Director of Public Prosecution & 2 others;* Criminal Appeal No. 7 of 2020, [2021] eKLR

Weblink: Judgment

Issue: Enforcement of the provisions of section 22 and 27 of the Computer Misuse and Cybercrime Act Number 5 of 2018 through private prosecution.

Legislation

- Sections 22 and 27 of the Computer Misuse and Cybercrime Act No. 5 of 2018

Facts

The appeal challenges the decision of the Trial Court denying the appellants leave to commence private prosecution. It was the Applicants' case that the second and third respondents (Paul Werunga and Gilbert Kipyegon) had circulated false information against them, which was posted on various YouTube channels and Facebook websites and that caused them a lot of pain and suffering. As a result, they lodged a complaint at Bomet Police Station on 3 June 2020. The appellants additionally argued that the investigations were finished, that they were dissatisfied with the results, and that they had grounds to think that the prosecution had handled their case improperly.

They contended that the investigating officers did not address themselves with the provisions of sections 22 and 27 of the Computer Misuse and Cybercrime Act Number 5 of 2018. It was also their case that the investigations and report were predetermined and/or biased, as contents of their letter dated 30 June 2020 addressed to the first respondent's office remained unanswered. They urged that they followed up the matter with the Director of Public Prosecutions (DPP), but they declined to prosecute the second and third respondents. And that the failure of the DPP to prosecute the respondents resulted in a failure of public and private justice and that the DPP had abdicated its role as mandated under the Constitution of Kenya 2010.

The appellants prayed that they be allowed to commence private prosecution in a bid to ensure that victims of cyber harassment, cyber bullying and spread of false information are assisted by various government officers. That they be allowed to commence the private prosecution if the DPP was not willing to take up its constitutional mandate.

Decision of the court

The High Court considered the scope of the powers of the Director of Public Prosecutions and evaluated whether the appellants had met the threshold for grant of leave to institute private prosecution. It determined that there was indeed no legitimate expectation that all complaints investigated must lead to prosecution. It held that the appellants had failed to discharge their burden of proof to show that the Director of Public Prosecutions had abdicated its duty or that the decision not to charge was tainted with malice and ill will. The court therefore concluded that the appellants had failed to meet the threshold necessary for the grant of leave to institute private prosecution and, in the absence of evidence of any wrongdoing by the first respondent, it could not interfere with the first respondent's decision not to charge the second and third respondents.

MAURITIUS

Title: *Seegum J v The State of Mauritius* [2021] SCJ 162

Weblink: Judgment

Issue: Whether section 46(h)(ii) of the Information and Communication Technologies Act (ICTA) 2001 offends the principle of legality, implied in section 10(4) of the Constitution, which requires that in criminal matters laws must be formulated with sufficient clarity and precision to enable a person to regulate his conduct.

Legislation

- Sections 46(h)(ii) and 47 of the Information and Communication Technologies Act 2001
- Section 10(4) of the Constitution

Facts

The appellant was prosecuted before the intermediate court in breach of sections 46(h)(ii) and 47 of the Information and Communication Technologies Act 2001 ('the ICTA') for the offence of 'using an information and communication service for the purpose of causing annoyance'. The appellant pleaded not guilty at trial but was found guilty. He appealed against the judgment of the magistrate. The appellant submitted that section 46(h)(ii) offends the principle of legality, implied in section 10(4) of the Constitution, which requires that in criminal matters, any law must be formulated with sufficient clarity and precision to enable a person to regulate his conduct.

Decision of the court

Allowing the appeal, the Supreme Court declared section 46(h)(ii) of the Information and Communication Technologies Act (as it then stood) as unconstitutional and contrary to section 10(4) of the Constitution. It noted that the then section 46(h)(ii), which read as:

. *Any person who…uses an information and communication service, including telecommunication service, for the purpose of*

causing annoyance, inconvenience or needless anxiety to any person… shall commit an offence

was cast so widely that a wide array of unacceptable communications (child pornography) to innocuous communications from the view of the ordinary citizen, may arguably have fallen within the realm of the Act. The Act did not make it clear to the ordinary citizen what might cause annoyance and what acts and omissions would render him liable to prosecution. It therefore breached the principle of legality implied under section 10(4) of the Constitution and deprived the citizen of the protection of the law. The court also differentiated between Mauritian law and the English and Indian provisions, in which the requirement of knowledge of a false electronic communication made the law more objectively ascertainable by the courts and by the citizens. The court quashed the appellant's conviction and sentence.

NAMIBIA

***State v Shipandeka* (CC 8 of 2018) [2020] NAHCMD 26 (30 January 2020)**

Weblink: Judgment

Issue: Theft by false pretences; money laundering.

Legislation

- Prevention of Organised Crime Act 29 of 2004

Facts

Using his workplace system, the defendant created fictitious client accounts using his girlfriend's bank account. There were potential losses of 2.4 million Namibia dollars (N$). The defendant pleaded guilty to all charges and was convicted on five counts of theft by false pretences. The sixth count was in respect of a statutory offence of money laundering in contravention of section 4(b)(i), read with section 1, 8 and 11 of the Prevention of Organised Crime Act 29 of 2004 as amended.

The High Court proceeded to sentencing. In doing so, it considered the nature of the offences, his personal circumstances and the interest of society.

Decision of the court

The High Court ruled that the defendant deliberately planned to commit the crimes and had time to reflect and change his mind. His actions were said to be premeditated, blatant and greedy. The court reiterated the seriousness of the offences, especially given that he was in a position of trust as he was employed as an information technology (IT) technician. It also emphasised that while the accused was a first-time offender, given that Namibia had been experiencing a large, alarming number of cases involving false pretences, the court needed to deter this conduct both in the public and private sectors. For this reason, given the severity of the crime, a custodial sentence was unavoidable under the circumstances, and he was sentenced to six years' imprisonment.

The sentences handed down were as follows: counts one to five: six (6) years' imprisonment, of which a period of two (2) years was suspended for five (5) years on condition that the defendant was not convicted of an offence of which dishonesty was an element, committed during the period of suspension; count six: three (3) years' imprisonment; the sentence on the 6th count was ordered to run concurrently with the sentence on the first to fifth counts.

Title: *S v Koning* (14 of 2010) [2017] NAHCMD 274 (29 September 2017)

Weblink: Judgment

Issue: Sentence for 18 counts of fraud, committed as an administrative clerk against her employer, through falsifying invoices.

Case law

- *S v Sadler* [2000] (1) SACR 331 (SCA)

Facts

The defendant worked as an administrative clerk at a business where she generated invoices on the computer. Following an investigation, it was discovered that the defendant owned the reprint history code and had defrauded the employer of N$1,808,399.33 by creating fictitious cigarette bills.

The defendant pleaded guilty and was convicted on 18 counts of fraud.

Decision of the court

The court proceeded to sentence. The court took into account the accused's personal circumstance; the crime itself and the interests of society. The court also gave regard to the objectives of punishment such as deterrence, prevention,

reformation and retribution. On the accused's circumstances, the length of time passed since arrest and the accused's children, and it being a first offence were noted. On the crime itself, the court considered the monetary loss of ±N$1,808,399.33. The court then turned to the interests of society. The court commented that the 'wellbeing of businesses is highly desired by the communities in order to deliver the required services to the people' and that 'society also expects employees of businesses to execute their duties diligently in order to maintain their own job security as well as the anticipation of possible new recruitments' [6]. Given that she had defrauded her own employer, this was a serious crime, and the law could not give the wrong impression that prison was only for those who commit violence crimes and not white-collar crimes.

The court sentenced the defendant to twelve (12) years imprisonment of which seven (7) years was suspended for a period of five (5) years on condition that she was not convicted of fraud committed during the period of suspension.

NIGERIA

Title: *Solomon Okedara v Attorney General of the Federation (2019)*

Weblink: Court of Appeal Judgment | Federal High Court Judgment | Notice of Appeal

Issues: The main issues for the court were the following.

- Whether section 24(1) of the Cybercrime Act 2015 was sufficiently defined and clear as to meet the requirements of a criminal offence under sections 36(12) and 39 of the Constitution.
- Whether section 24(1) of the Cybercrime Act (CA) 2015 infringed upon freedom of expression and fair hearing as protected by sections 36 and 39 of the Constitution.
- Whether the provisions of section 24(1) of the CA 2015 were within the permissible restrictions stipulated in section 45 of the Constitution.

Legislation

- Section 24(1) of the Cybercrime (Prohibition, Prevention, etc.) Act 2015
- Sections 39, 36(12) and 45 of the Constitution

Facts

Solomon Okedara, a legal practitioner in Nigeria, filed an application before the Federal High Court in Lagos challenging the constitutionality of section 24(1) of the Cybercrime (Prohibition, Prevention, etc.) Act 2015. Section 24(1) made the following an offence.

. *Any person who, knowingly or intentionally sends a message or other matter by means of computer systems or network that*

(a) *Is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or*

(b) *He knows to be false, for the purpose for causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent: commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.*

Solomon Okedara argued that section 24(1) lacked a clear definition of the offense as it was vague and overbroad. He also argued that it threatened his right to freedom of expression (protected by section 39 of the Constitution) and a fair hearing (protected by section 36(12) of the Constitution).

Decision of the court

Federal High Court

- The court found section 24(1) of the Cybercrime Act 2015 was clear and defined and not in conflict with section 36(12). The court determined that section 24(1) was in the best interest of the generality of the public.
- The court noted that cybercrime was incapable of direct definition.
- The Act was in the interest of defence, public safety, public order, public morality and public health. It did not fall within the permissible restrictions under section 45 of the Constitution.

Court of Appeal

Mr Okedara appealed to the Court of Appeal. The Court of Appeal affirmed the Federal High Court judgement, dismissing the appeal.

Main issues

Was section 24(1) of the CA 2015 unconstitutional?

- The court noted that freedoms under section 39 of the Constitution were guaranteed, but not open-ended or absolute. They were qualified and subject to restrictions as set out in section 45 of the Constitution.
- The court stated that the legislature had the power to enact laws that were reasonably justifiable in a democratic society and that such laws should not be declared invalid because they appeared to be in conflict with the rights and freedom extended to citizens under the Constitution.

Was section 24(1) of CA 2015 in conflict with section 39 of the Constitution and words such as 'grossly offensive', 'indecent', obscene' or 'menacing character' not given a clear definition in the act?

- Both the provisions of the CA 2015 and section 45 of the Constitution set out to protect the privacy rights of citizens. Therefore, the intention of the legislature in enacting the CA 2015 was in accord with the provisions of section 45 of the Constitution.

Did section 24 of the Act satisfy the requirements of section 36(12) of the Constitution?

- Section 24(1) CA 2015 was not in conflict with the provisions of sections 36(12) and 39 of the Constitution.
- The court reasoned that the words of section 24(1) of the Act were 'explicit and leave no room for speculation or logical deductions' [p.27]. The offence was clearly defined and the penalty clearly stated.

RWANDA

Title: *Ikiza Ry' Urubanza RP/ECON 00002/2020/TGI/GSBO*

Weblink: Judgment

Issue: Unauthorised access to a computer; unauthorised modification of computer; theft.

Legislation

- Articles 16, 17 and 18 of Law N° 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes 2018
- Articles 166 and 224 of Law N° 68/2018 of 30/08/2018 determining offences and penalties in general

Facts

Twenty-two (22) defendants from Kenya were alleged to be involved in an organised scheme of attempting to steal millions from a major bank operating in Rwanda. Equity Bank had received notification that an organised criminal group were intending to steal money from them, as they had done in Kenya and Uganda.

The bank contacted the Rwanda Investigation Bureau (RIB), which found that the group had planned to execute a scam using customers' ATM cards through an application called Em Cert ID App. The defendants were arrested at a branch of the bank after attempting to steal from 23 accounts. Eight schemes were successful, leading to losses of 2,944,283 Rwanda francs (RF) in total.

All 22 defendants were each charged with unauthorised access to a computer or a computer system data, access to data with intent to commit an offence, unauthorised modification of computer or computer system data, theft, and formation of or joining a criminal association contrary to the Prevention and Punishment of Cyber Crimes 2018.

Decision of the court

The court discussed each defendant separately. The central issue for most of the defendants was the mental element: whether the defendant came to Rwanda with the intention of committing the crime, or whether they knowingly participated in actions for the purpose of committing the crime.

All defendants were convicted of all counts and sentenced to eight years' imprisonment each.

The court further ordered all defendants to jointly pay the amount of loss to Equity Bank of RF2,994,783. Each defendant was also ordered to pay Equity Bank a fee of approximately RF100,000, for the system expert consultation system review, travel expenses, maintenance expenses and tickets

of these experts, compensation for the losses incurred by Equity Bank, and a lawyer's fee.

SEYCHELLES

Title: *R v ML & Ors Cr S 63/19*

Weblink: Judgment

Issue: Whether the accused were guilty of 26 counts of sexual assault, extortion, possession of indecent photographs, possession of prohibited visual recordings, procuring or attempting to procure by way of threats or intimidation a girl to have unlawful carnal connection and recruiting, harbouring, transferring and receiving a child knowingly or recklessly disregarding that the person is a child for the purpose of exploitation contrary to the Penal Code and Prohibition of Trafficking in Persons Act (PTPA).

Legislation

- Section 5(1)(b), section 130(1), (2)(d), (3)(b), (4)(b), section 135(1), section 157, 157A, 157C, 157E of the Penal Code
- Section 3(1)(b) and 3(1) of the Prohibition of Trafficking in Persons Act 2014 (PTPA)

Facts

Three men were charged with 26 counts of sexual assault, extortion, possession of indecent photographs, possession of prohibited visual recordings, procuring or attempting to procure by way of threats or intimidation a girl to have unlawful carnal connection and recruiting, harbouring, transferring and receiving a child knowingly or recklessly disregarding that the person is a child for the purpose of exploitation.

The claimant, a 17-year-old student, made a complaint to the police that a person on Facebook was threatening her with exposing indecent images of herself engaging in sexual activities unless she had sex with him. The first defendant, the primary perpetrator who planned and executed the crimes, lured and groomed young girls using Facebook, promising them modelling jobs and money over a period of four years. After he received nude pictures from the victims, the first defendant blackmailed the victims by threatening to expose their identity if they refused to engage in sex with him and others. Following a 'sting' meeting, the first defendant was arrested and a number of hard drives, mobiles, pen drives and laptops were seized. On these were found images, texts and videos luring and engaging in sex with the young girls and of the other three defendants. The second defendant was a police officer of five years' service at the time of the offence; he pleaded guilty pursuant to section 130(1) for sexual assault as he had sexual intercourse with one of the victims, who was 14 years of age. The third defendant pleaded guilty to penetration of an orifice, the mouth, and pursuant to section 130(4)(b).

Decision of the court

The court found all three accused guilty of all 26 counts of the Penal Code.

In sentencing the three defendants, the court took into consideration that all defendants had pleaded guilty, thereby saving the victims the trauma of reliving the trauma they had endured in a lengthy criminal trial.

Defendant one was found guilty of counts 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 20, 21, 22, 24, 25 and 26 of the Penal Code. The court applied the principle of totality, giving a sentence of 25 years in prison. It drew on case law on the totality principle from Kenya, Canada, the United Kingdom and Australia, ordering some of sentences to run concurrently and some to run consecutively. The first defendant was also placed on the Sexual Offenders Register and all his actions with children closely monitored.

The second defendant was not sentenced to the minimum mandatory term of 14 years' imprisonment because there was no indication that he had engaged with the first defendant in any of the other offences. Given that he was a police officer at the time, he was entrusted by the state to protect children from such reprehensible and degrading acts and given a sentence of 12 years' imprisonment.

The third defendant was convicted on count 16 for the offence of sexual assault contrary to section 130(1) and (2)(a) of the Penal Code. Given that he was only 18 years of age at the time of the offence, the court found that he was impressionable and led on by defendant one. As such, he was sentenced to a term of eight years' imprisonment.

The court emphasised the need to balance the serious nature of the crimes, mitigating factors, the public interest and the different circumstances of the offenders. The court further emphasised the

irreparable harm that such crimes inflict on children and warned of the increase of offences of this nature, noting a need for specialised cybercrime laws and investigating units to respond to this.

SOUTH AFRICA

Title: *Fourie v Van Der Spuy & De Jongh Inc And Others* 2020 (1) Sa 560 (Gp)

Weblink: Judgment

Issue: Electronic fraud; hacking.

Legislation

- Section 23(1)(a) of the Attorney's Act 53 of 1978

Facts

The Applicant had engaged the services of a law firm (the first respondent) to keep certain monies belonging to him in the firm's trust account until further instruction. The Applicant's email account was subsequently hacked; the hackers sent an email to the second respondent (an attorney at the firm) asking to make payments into several identified bank accounts. The respondents paid the monies into the accounts without verifying the transactions with the Applicant.

Decision of the court

The High Court found that the second respondent, by transacting via email without employing any measures to ensure that both she and her client would not fall victim to fraud and knowing full well that it was prevalent in her profession, acted negligently and failed to exercise the requisite skill, knowledge and diligence of an average practising attorney, and thus failed to discharge her fiduciary duty to her client. The second respondent had failed to account to her client for the funds held in the firm's trust account on their behalf. It was no defence to claim that payments were made erroneously.

The respondents were held jointly and severally liable for the loss suffered by the Applicant. They were ordered to pay the loss suffered by Mr Fourie with interest of 1,744, 599.45 rand (R).

Title: *Brown v Economic Freedom Fighters and Others* (14686/2019) [2019] ZAGPJHC 166

Weblink: Judgment

Issue: Cyber harassment.

Legislation

- Clauses 2, 3, 6 and 8 of the Electoral Code as contained in Schedule 2 to the Electoral Act 73 of 1998 (the 'Act') and section 94 of the Act

Facts

On 5 March 2019, Karima Brown, South African political journalist, sent a WhatsApp message to a group created by Mbuyiseni Ndlozi, the national spokesperson of the Economic Freedom Fighters (EFF), a South African political party. Brown claimed to have intended to send the message to her colleagues, not the group it was sent to. The message referred to an EFF event. Brown wrote: 'Keep an eye out for this. Who are these elders? Are they all male and how are they chosen? Keep watching brief.'

The president of EFF, Julius Malema, published a screenshot of the message on Twitter to his 2.38 million followers. The image included Brown's name and personal mobile telephone number.

Ndlozi released a statement on behalf of the EFF claiming that Brown was an operative for the South African ruling party, the African National Congress (ANC), and was not a legitimate journalist. The EFF also published a statement on its Facebook page, repeating these claims.

Following this, Brown received a wave of threatening phone calls and written threats on Twitter and WhatsApp from self-proclaimed EFF supporters, which included threats of rape, violence and death.

Decision of the court

The central issue for the court was whether EFF's failure to condemn its supporters' threats to and harassment of Brown, and failure to tell them to refrain from future harassment, was an infringement of the Electoral Code.

The South Gauteng High Court in Johannesburg ruled that EFF had contravened clauses 3 and 8 of the Electoral Code contained in Schedule 2 to the Electoral Act 73 of 1998 and section 94 of that Act. There was a failure of a political party to condemn its supporters' harassment of and threats against the journalist and to adhere to its obligations to respect the rights of women and of the media under the Electoral Code.

The EFF and its leaders needed to take reasonable steps to condemn and stop the harassment experienced by the journalist.

UGANDA

Title: *Stella Nyanzi v Uganda* [2020] UGHCCRD 1 (20 February 2020)

Weblink: Judgment

Issue: Enforcement of the offences of cyber harassment contrary to section 24(1), (2)(a) of the Computer Misuse Act 2011 and the offence of offensive communications contrary to section 25 of the Computer Misuse Act, Act 2 of 2011.

Legislation

- Section 24(1) and 24(2)(a) of the Computer Misuse Act (CMA) 2011
- Section 25 of the Computer Misuse Act, Act 2 of 2011
- Article 28(3)(d) of the Constitution of the Republic of Uganda

Facts

The appellant, Dr Nyanzi, a medical anthropologist and former research fellow at Makerere University, was charged with two counts before the Buganda Road Chief Magistrate's Court: cyber harassment contrary to section 24(1), (2)(a) of the Computer Misuse Act 2011, and offensive communications contrary to section 25 of the CMA 2 of 2011.

The appellant had posted on her Facebook page the following.

- *Yoweri…I wish the smelly and itchy cream-coloured candida festering in Esteri's cunt had suffocated you to death during birth.*
- *Yoweri…I wish the acidic pus flooding Esteri's cursed vaginal canal had burnt up on your unborn fetus.*
- *Yoweri…I wish the infectious dirty-brown discharge flooding Esteri's loose pussy had drowned you to death.*

Charges were brought for the comments being obscene, lewd or indecent, and transmitted over the internet to disturb the peace, quiet or right to privacy of His Excellency the President of Uganda, Yoweri Kaguta Museveni, with no purpose of legitimate communication.

The appellant was tried by the lower court who handed down its judgement on 1 August 2019, finding the appellant guilty of the offence of cyber harassment contrary to section 24(1), (2)(a) of the Computer Misuse Act, Act 2 of 2011, in count one. The appellant was acquitted of the offence of offensive communications contrary to section 25 of the Computer Misuse Act, Act 2 of 2011, charged in count two.

In finding the case against the appellant on count one of the offence of cyber harassment contrary to section 24(1), (2)(a) of the Computer Misuse Act of 2011, the lower trial court held that the statements made in the posts found on the Facebook account of the appellant were obscene, lewd and indecent on the basis on the Hicklin Test for obscenity, as established by the English case *Regina v Hicklin* [1868] LR 3, QB 360.

Decision of the court

The High Court heard the appeal and granted it on grounds that the Trial Court lacked jurisdiction to entertain the matter and assumption of jurisdiction, rendering the trial a nullity. It also determined that the appellant was not afforded a fair trial for reasons that she was totally excluded from physical appearance in court without her consent or notification, which violated the appellant's rights under Article 28(3)(d) of the Constitution of the Republic of Uganda, guaranteeing the right of a person charged with a criminal offence to be permitted to appear before the court in person.

The High Court granted the following orders.

- The trial, procedure, judgment and all the findings of the lower court were hereby declared a nullity with the appellant, set aside and the appellant acquitted forthwith.
- The conviction against the appellant was also hereby quashed.
- The appellant was acquitted and ordered to be released from custody unless being held for any other lawful charges.
- Any right of appeal by any aggrieved party must be exercised within the meaning of appropriate law, including section 132 of the Trial on Indictment Act and any other relevant law including the Magistrates Court Act.

Title: *Uganda v Nsubuga & Ors* (HCT-00-AC-0084-2012) [2013] UGHCACD 12 (3 April 2013)

Weblink: Judgment

Issue: Electronic fraud.

Legislation

- Sections 12(2), 15(1), 19 and 20 of the Computer Misuse Act (CMA) 2011
- Sections 191(1)(a) and 203(e) of the East African Community Customs Management Act 2009
- Protection from Harassment Act 1997 (UK)
- Harmful Digital Communications Act 2015 (New Zealand)
- The Intimate Images and Cyber-Protection Act, NSN 2017 (Nova Scotia)

Case law

- *Merrifield v Canada (Attorney General)* 2017 ONSC 1333; 2019 ONCA 205

Facts

The Uganda Revenue Authority (URA) suspected its computer systems were compromised, leading to losses of 2,461,447,275 Uganda shilling (USh) and 78 cents. The URA began internal investigations. Following a tip off, four defendants were arrested in a vehicle in the proximity of the URA at Nakawa. Three laptops, an inverter, an external hard disk and other electronic paraphernalia were seized. The four defendants (A1–A4) were jointly indicted on six counts:

Count one: unauthorised use and interception of computer services, contrary to sections 15(1) and 20 of the Computer Misuse Act. The defendants allegedly made changes on the URA database, making it appear the changes were made by authorised persons. Computers not registered on the URA domain were used. A1 and A4 were convicted; A2 and A3 were acquitted on count one.

Count two: electronic fraud, contrary to section 19 of the Computer Misuse Act. Communications between A1 and A4 showed an objective to deceive those in IT security at the URA by accessing its computer system using spyware for unlawful and unfair gain. A1 and A4 were found guilty. A2 and A3 were acquitted.

Count three: unauthorised access to data, contrary to sections 12(2) and 20 of the Computer Misuse Act. The defendants allegedly intentionally and without authority interfered with data in a manner that caused the data to be modified and to an extent damaged. The court found A1 and A4 guilty and acquitted A2 and A3.

Count four: producing, selling or procuring, designing and being in possession of devices, computers, computer programmes designed to overcome security measures for protection of data, contrary to sections 12(3) and 20 of the Computer Misuse Act. There was evidence that A4 made purchases of spyware and that A1 and A4 were in possession of spyware. A1 and A4 were convicted on this count and A2 and A3 were acquitted.

Count five: unauthorised access to a customs computerised system, contrary to section 191(1)(a) of the East African Community Customs Management Act 2009. Evidence of interference with the URA computer system and modification and alteration to it was found. A1 and A4 were convicted on this count.

Count six: fraudulent evasion of payment of duty, contrary to section 203(e) of the East African Community Customs Management Act 2009. The accused persons were alleged to be responsible for the loss of USh2,461,447,275 and 78 cents, being the amount not paid in duty. The court held that despite some rare cases involving taxation where strict liability is imposed and therefore the burden of proof rests on the defendant, this was not one of those cases. The prosecution bore the burden to prove the defendants' knowledge or intent. The prosecution did not tender such evidence to prove this, nor how the sum was come by, nor that the defendants acted in concert. None of the defendants were found guilty under count six.

Decision of the court

In sum, A1 and A4 were found guilty on counts one to five and acquitted on count six. A2 and A3 were acquitted of all counts.

The court discussed the extraction of electronic evidence. In this instance, the Encase solution was employed. Forensic professionals that need to carry out effective, forensically sound data collection and investigations that are stated to be repeatable and defensible employ the Encase solution. Data are collected from a wide range of devices, and disc

level forensic analysis reveals relevant evidence. Encase forensic specialists preserve the forensic integrity of their evidence while doing so (21). The court cited the case of *Armstrong v Executive Office of the President, IF.3d 1274 (D.C.Cir 1993*), where it was found that a hard copy of electronic evidence would not have all the information, and that a digital and hard copy should both be given as evidence – as was done in this case.

In deciding the sentence, the court considered the young age of A1 and A4, and that they had families and were breadwinners. However, it balanced this with the need for a stiff sentence as the actions of the accused 'resulted in tremendous loss to the exchequer of URA and compromised the security system of the country' (22). The court also considered the lack of previous record, their remorse and time spent on remand. The court declined to invoke section 20 of the CMA 2011, which renders the defendants liable to life imprisonment on counts one, three and four. A1 and A4 were each sentenced to 12 years' imprisonment on count two, 8 years' imprisonment on counts one, three and four, all custodial sentences to run concurrently, and a fine of US$4,500 on count five.

Title: *Uganda v Ssentongo & 4 Ors* (Criminal Session Case 123 of 2012) [2017] UGHCACD 1 (14 February 2017)

Weblink: Judgment

Issue: Embezzlement, electronic fraud.

Legislation

- Section 19(b)(i) of the Anti-Corruption Act (ACA) 2009
- Section 17, 19 of the Computer Misuse Act 2011
- Section 309 of the Penal Code Act

Facts

A1-A5 are five former employees of Uganda's leading telecom company allegedly swindled money amounting to USh10 billion. Using the company's previous mobile money computer system, the defendants created billions of shillings and wired them to their mobile money accounts, which were created by themselves before resigning from their jobs. The A1 manipulated the telecom's system to create non-existent e-money (float) and cashed it straight into circulation. He also created four usernames to create journals on the company's mobile money accounts with the help of his co-defendant (A2). Four of the defendants left the company in close succession, which raised suspicion of criminal activity. Investigations found that they had committed malpractices as their usernames appeared on the fraudulent transactions. Evidence showed that the first defendant abused the trust expected of him by manipulating the system to steal money from the mobile platform in conspiracy with his co-defendants.

Decision of the court

The defendants were charged on eight counts including embezzlement contrary to section 19(b)(i) of the ACA 2009, electronic fraud contrary to section 19 of the Computer Misuse Act 2011, unauthorised disclosure of access codes contrary to section 17 of the Computer Misuse Act 2011, and conspiracy to defraud contrary to Section 309 of the Penal Code Act. A1 and A2 were convicted of charges of embezzlement contrary to section 19(b)(i) of the ACA 2009 and conspiracy to defraud contrary to section 309 of the PCA, Cap 120. A1 was further convicted of electronic fraud contrary to section 19 of the Computer Misuse Act 2011. A3, A4 and A5 were acquitted of the charges against them.

TANZANIA

Title: *Werdy Mwaipopo v R* (Criminal Appeal 108 of 2020) [2020] TZHC 3579 (05 October 2020)

Weblink: Judgment

Issue: Enforcement of the offence of publishing racist and xenophobic motivated insult contrary to section 18(1) and (2) of the Cybercrimes Act No. 14 of 2015.

Legislation

- Section 18(1) and (2) of the Cybercrimes Act No. 14 of 2015

Facts

In the District Court, the appellant was charged and convicted of the offence of publishing racist and xenophobic motivated insult contrary to section 18(1) and (2) of the Cybercrimes Act No. 14 of 2015. The appellant was alleged to have published through his Facebook account a picture of a pig with a message

stating: 'Mtume Muhammad Anawatakia Mchana Mwema Wadau.' Following the conviction, he was sentenced to three years and six months in custody.

The appellant appealed to the High Court on seven grounds, which can be conveniently reduced into two: that the prosecution case was not proved beyond reasonable doubt; and that there was no ruling on establishment of a prima facie case against the appellant.

Decision of the court

The appeal was partially allowed.

The court (Mongella J) was of the view that the concern of the trial magistrate that the offence committed 'might raise negative sentiments' was not sufficient explanation on the imposition of the sentence beyond the minimum sentence provided under the law. In addition, it found that section 18(2) provided for an option of a fine, which option the trial magistrate did not offer to the appellant or give reasons why the same was not available to the appellant. For these reasons, the court upheld the offence but varied the sentence issued by the trial court to a fine of three million (3,000,000/-) Tanzanian shillings (TSh) or in default to serve an imprisonment term of one year.

Title: *Director of Public Prosecutions v Abdul Mohamed Omary Nondo* (RM Criminal Appeal 10 of 2019) [2019] TZHC 195 (23 December 2019)

Weblink: Judgment

Issue: Enforcement of the offences of publication of false information contrary to section 16 of the Cybercrimes Act (No. 14 of 2015) and giving false information to a person employed in the public service contrary to section 112(a) of the Penal Code Chapter 16 Revised Edition 2002.

Legislation

- Section 16 of the Cybercrimes Act No. 14 of 2015
- Section 112(a) of the Penal Code, Chapter 16 Revised Edition 2002

Facts

The respondent, Abdul Mohamed Omari Nondo, was charged before the Resident Magistrate's Court of Iringa on two offences: publication of false information contrary to section 16 of the Cybercrimes Act (No. 14 of 2015) and giving false information to a person employed in the public service contrary to section 112(a) of the Penal Code Chapter 16 Revised Edition 2002. The trial court found that the appellant, the Director of Public Prosecutions, had not proved the allegations beyond reasonable doubt.

The respondent was consequently cleared of the charges and acquitted. The appellant was dissatisfied with the judgment of the learned trial resident magistrate and had come to this court to fault its validity.

Decision of the court

The court upheld the Trial Court and dismissed the appeal on similar grounds that the alleged offences had not been proved beyond reasonable grounds.

Title: *Jamii Media Company Ltd v The Attorney General and Another* [2016]

Weblink: Judgment

Issue: Whether the provisions of sections 32 and 38 of the Cybercrimes Act No. 14 of 2015 were unconstitutional for offending the provisions of Articles 13(6)(a), 16 and 18(1)(2) of the Constitution of the United Republic of Tanzania 1977.

Legislation

- Sections 32 and 38 of the Cybercrimes Act 2015
- Section 4 of the Basic Rights and Duties Act, Cap 3
- Rule 4 of the Basic Rights and Duties (Practice and Procedure) Rules 2014
- Articles 13, 16 and 18 of the Constitution of the United Republic of Tanzania 1977

Facts

The petitioners owned a website where users were able to post comments on social, economic or political matters anonymously. The petitioners stated they had received a number of 'disclosure orders' demanding users' information from the police under section 32 of the Cybercrimes Act 2015. The petitioners responded in writing to these disclosure orders, asking the police to disclose the nature of criminal investigations they were conducting, so as to justify the submission of the information requested. The police threatened prosecution under section 32 of the Cybercrimes Act 2015.

The petitioners challenged whether section 32 of the Cybercrimes Act 2015 was constitutional, arguing it interfered with the right to privacy protected by Article 16 of the Constitution and freedom of expression provided for by Article 18. The petitioners further contended that section 38 of the Act, which enabled the police to condemn service providers without giving the opportunity for representations, including by confiscating electronic devices, infringed upon Article 13(6)(a) of the Constitution protecting the right to be heard.

The police argued that technological advancement had posed legal and operational challenges to law and order as police were unable to respond adequately to crimes associated with the digital world. In their view, the Cybercrimes Act was enacted to protect the victims of cybercrime, arrest and prosecute the guilty.

Decision of the court

The court held that there was no suggestion that the Cybercrimes Act had not been lawfully enacted. A rule of law was only arbitrary if it had not been lawfully enacted by Parliament, or it did not appeal to reason. Section 32(4) of the Act did not empower the police to take away computer devices and the petitioner was only obliged to print out information requested for it to be taken away by investigators. The petitioner had the option to seek ex parte court intervention under section 32(3) and section 36 if disclosure of information was not voluntary. In determining the issue, the court balanced the right to privacy against the wider interest of the public by applying the reasonableness test. The court examined provisions of Articles 19(2) and (3) of the International Covenant on Civil and Political Rights and other national laws to conclude that section 32 of the Act was within the proportional restrictions permitted in both national and international jurisprudence. The court held that the petitioner had not proved that neither section 32 nor section 38 of the Act was unconstitutional. The petition was dismissed.

CASE ANALYSES – ASIA

BRUNEI DARUSSALAM

Title: *Public Prosecutor v Norhayati Binti Hj Zaini* (2017) ICCT/9/2017

Weblink: Judgment

Issue: Breach of trust and computer misuse.

Legislation

- Section 408 of the Penal Code
- Section 4(1) and section 10 of the Computer Misuse Act

Facts

The defendant had been employed by the Baiduri bank for 15 years prior to her 3 years as assistant manager. She oversaw the bank tellers in her capacity as assistant manager, gave approval to certain transactions, and oversaw the bank branch's cash operations. The defendant asked multiple bank tellers to access the system with their identification (IDs) and complete transactions as she lacked authorisation to do so. The defendant had done this in order to aid in the commission of the crime of causing a computer to carry out a task that secured access to a programme stored on the bank's computer server with the intention of utilising such access to commit a crime involving criminal breach of trust. She stole 84,928.90 Brunei dollars (Br$) from four bank accounts that were handled by the bank. The defendant entered guilty pleas to two counts under section 4(1) of the Computer Misuse Act, three counts under section 10 of the Computer Misuse Act, and one count of criminal breach of trust under section 408 of the Penal Code.

Decision of the court

The court found the defendant guilty on all six counts. In its sentencing, the court reiterated that the offence of criminal breach of trust and offences committed under the Computer Misuse Act are serious. She had grossly misused her position of authority over bank staff in the commission of the offence. The court emphasised that a deterrent sentence should be imposed to reflect the gravity of the offence committed. She was found guilty on all five charges and sentenced to be imprisoned for three years and six months.

INDIA

Title: *Christian Louboutin SAS v Nakul Bajaj & Ors* CS (Comm) No. 344/2018, 2 November 2018

Weblink: Weblink

Issue: Whether an e-commerce website was classified as an intermediary under section 79 of the Information Technology Act 200, and therefore protected by the safe harbour defence in relation to a claim under section 29 of the Trademark Act 1999.

Legislation

- Information Technology Act 2000, section 79
- Trademark Act 1999, section 29

Facts

The claimant, luxury fashion brand Christian Louboutin, brought a claim against an e-commerce retailer, for selling Louboutin products through third-party sellers and using their trademarks, allegedly in breach of the claimant's intellectual property rights. The defendants claimed they were merely an intermediary and therefore not liable for trademark infringement, as the safe harbour defence under section 79 of the IT Act applied. The claimants argued that the defendants performed a role greater than that of an intermediary and were liable.

Decision of the court

In a judgement representing the first of its kind, the Delhi High Court determined that the defendant e-commerce platform was performing an active role in the sale of the claimant's goods and, as such, was more than an intermediary. The safe harbour defence under section 79 of the IT Act 2000 therefore was not available to them.

The defendants would thus be at risk of liability for encroachment on the claimant's intellectual property (IP) rights wherever counterfeit products were sold through its website.

Considering the case of *Kapil Wadhwa v Samsung Electronics* FAO(OS) 93/12, the court held that meta-tags were a trademark infringement.

In this case, no Louboutin products had actually been sold. The court made no order for damages/rendition of accounts or costs. However, the court did provide a list of actions for the defendant in the management of its website, including a requirement to obtain authentication from each of its sellers that the merchandise was certifiable as genuine.

Title: *The State of Odisha v Jayanta Kumar Das* [2017] (*Puri Sub-Divisional Judicial Magistrate Court) No.1739/2012

Weblink: Judgment

Issue: Forgery, forgery for harming reputation, publication of obscene content and defamation, contrary to sections 292, 465 and 500 of the Indian Penal Code1860. Identity theft, sending of offensive messages, publishing or transmitting obscene material in electronic form, and publishing or transmitting of material containing sexually explicit acts, etc., in electronic form, contrary to sections 6(C), 66C, 67(A) and 79(A) of the Information and Technology (Amendment) Act 2008.

Legislation

- Indian Penal Code 1860
- 66(C)/67/67(A) of Information and Technology (Amendment) Act 2008

Facts

Odisha's first conviction for cyber pornography. The defendant uploaded photos of a married woman on a pornographic website in 2012 and created fake profiles for sharing widely by groups online. The woman was the wife of a journalist who had previously written against the defendant.

Decision of the court

The court handed down a sentence of six years' imprisonment and a fine of 9,000 Indian rupees (Rs) (multiple sentences to run consecutively).

Title: *Mukul v State of Punjab* (2018) High Court of Punjab and Haryana at Chandigarh

Weblink: Judgment

Issue: Whether electronic evidence (WhatsApp messages) should be considered by the court when deciding whether a person other than the accused could be summoned to the court under section 319 of the Code of Criminal Procedure.

Legislation

- Section 319 of the Code of Criminal Procedure

Facts

The victim, deceased, had been threatened by the defendant who demanded an illicit relationship, otherwise he would post nude photographs of the victim online. The victim's body was found in a river following a suspected suicide. During the trial of the defendant, further persons were accused, and an application was moved by the complainant to summon the additional accused. That application was allowed and was the subject of this challenge. WhatsApp messages showed the victim had contact with the additional accused, allegedly supporting the case that the additional accused had gang raped the victim, leading to her suicide. The court considered whether the messages should be considered in the proper application of section 319 of the Code of Criminal Procedure, which allows for persons other than the accused to be summoned to the court.

Decision of the court

The court found that the word 'evidence' should be understood in its wider sense, both at the stage of trial and even at the stage of inquiry. This means that the power to proceed against any person after summoning him or her can be exercised on the basis of any such material as brought forth before it. The WhatsApp messages were allowed to be considered when deciding if the conditions to summon additional accused persons were satisfied.

The court ultimately upheld the petition against summons. It held that although the WhatsApp messages were to be considered as evidence, on these facts, the conditions for summoning the additional persons were not satisfied.

Title: *Nupur Ghatge v The State Of Madhya Pradesh* (2022) Madhya Pradesh High Court MCRC-52596-2020

Weblink: Judgment

Issue: Whether the court should allow the appeal of the appellant's conviction contrary to section 67B of the Information Technology Act 2000, on the basis that he did not forward, transmit or create the pornographic material, and that the victim did not come forward to complain of said material.

Legislation

- Section 67B of the Information Technology Act 2000
- Section 84 of the Code of Criminal Procedure 1973
- Section 482 of the Indian Penal Code

Facts

It was alleged that the applicant, a 19-year-old student, uploaded a child pornography video and photographs on his Instagram account from a mobile number that was registered in the name of his father. Investigators also found WhatsApp chats of the applicant with the victim which clearly indicated his involvement in child pornography. Following investigations, he was found guilty on one count of publishing or transmitting material depicting children in sexually explicit acts in electronic form, contrary to section 67B of the Information Technology Act 2000. He appealed his conviction arguing that he did not forward the material to any other account and that he played no role either in transmitting the said pornography or creating the video or photographs. He also argued that as no victim had come forward to complain of the transmission of the pornography, he could not be prosecuted.

Decision of the court

Dismissing the application, the court upheld the convictions of the lower court. It was clear from the electronic communications that the applicant was involved in the pornographic activities. Therefore, the provision of section 67B of the Act 2000 was applicable, as section 67B of the Act also includes records in any electronic form of abuse or that of others pertaining to sexually explicit acts with children. The submission that in the absence of any complainant, the applicant could not be prosecuted, was held to be misconceived. The applicant's claim that he was 19 years old and still a young boy had no legal basis and was based on morality.

MALAYSIA

Title: *Toh See Wei v Teddric Jon Mohr & Anor* [2017] 11 MLJ 67

Weblink: https://www.coursehero.com/file/73726787/Toh-See-Wei-v-Teddric-Jon-Mohr-Anorpdf/

Issue: Unauthorised access to information, contrary to the Computer Crimes Act (CCA) 1997.

Legislation

- Computer Crimes Act 1997

Facts

The defendant allegedly hacked into the plaintiff's email account and downloaded/printed out emails sent to third parties. There is no definition of 'hacking' under the CCA. However, the High Court in this case did shed some light in defining 'hacking' to mean 'unauthorised access to the computer system'. Commentators have criticised the CCA's vagueness in this regard.

Decision of the court

There was insufficient evidence to prove on the balance of probabilities that the email account was hacked.

Title: *Mohd Fahmi Redza Bin Mohd Zarin Lawan Pendakwa Raya dan Satu Lagi Kes* [2017] MLJU 516; [2020] 7 MLJ 399 (High Court)

Weblink: Summary

Issue: This case was an appeal on conviction of sending false communications via a social media application with intent to injure others, contrary to section 233(1)(a) of the Communications and Multimedia Act 1998.

Legislation

- Communications and Multimedia Act (CMA) 1998

Facts

A freelance graphic artist was convicted under section 233(1)(a) of the CMA 1998 for uploading a poster of a former prime minister as a clown to Facebook. He received a sentence of one month in jail and a fine of 30,000 ringgit (RM).

The convicted appealed on the basis that the upload amounted to parody or political satire, without any intention to annoy.

The court noted that while the convicted could not be barred from harbouring his own political views, as these were embodied in a communication, he could not maintain that the communication did not conflict with the law. The court emphasised that the

question was not whether it did annoy, but whether it was intended to. The court identified three criteria that the prosecution had to satisfy beyond reasonable doubt.

(a) MF used his FB page, an application service, to upload;

(b) the communication was false in nature; and

(c) the communication was intended to injure another.

Decision of the court

The High Court held that all three of the above conditions had been met in this case.

The court upheld the conviction but reduced the sentence to RM10,000, with imprisonment of one month in default.

Title: *PP v Mohamad Faezi bin Abd Latif* [2020] 5 LNS 42 (Sessions Court)

Weblink: Judgment

Issue: Ten charges of improper use of an application service by knowingly creating and initiating the transmission of obscene communications (sexually explicit images/videos) with intent to annoy another person, contrary to section 233(1)(a) of the Communications and Multimedia Act 1998.

Legislation

- Communications and Multimedia Act 1998

Facts

The defendant pleaded guilty to all charges.

The learned sessions court judge produced a helpful table consisting of sentences for those who had pleaded guilty at first instance under a section 233(1)(a) of the Communications and Multimedia Act 1998 charge.

Decision of the court

The offender was sentenced with a fine of RM5,000.00, with three months' imprisonment in default, on each charge, totalling RM50,000.00, with 30 months' imprisonment in default.

Title: *Nik Adib Bin Nik Mat v Public Prosecutor* [2017] MLJU 1831 (High Court Appeal)

Weblink: Judgment

Issue: The appellant was convicted of sending indecent and false photographs, contrary to section 233(1)(a) of the Communications and Multimedia Act 1998, and for possession of pornographic material, contrary to section 5(1)(a) of the Film Censorship Act 2002. He received the maximum sentence of one year's imprisonment for each offence. The appellant appealed the sentence.

Legislation

- Communications and Multimedia Act 1998
- Film Censorship Act 2002

Facts

The offender was convicted of sending indecent and false photos of cabinet leaders titled 'Pesta Bogel' on Facebook. He was also convicted under section 5(1)(a) of the Film Censorship Act 2002 for possession of 883 pieces of pornographic videos in his laptop. The Session Court sentenced him to the maximum sentence of one year's imprisonment for the first offence and another one year's imprisonment for the second offence.

On appeal, the High Court judge stated that 'cyber offences are serious offences, especially the offence at hand, as those offensive materials could be easily disseminated to the public at large within seconds at a touch of a button'. The judge agreed with the sessions court judge that public interest was of paramount importance and should supersede the interest of the accused. However, the learned High Court judge was of the view that the personal interest of the accused should not be disregarded.

Decision of the court

The High Court allowed the appeal against sentence. The learned High Court judge took into account the grounds submitted by the accused and held that the misdirection of the Session Court on imposing maximum sentence for a first offence warranted the appellate intervention. The judge stated a special consideration ought to be given so that the accused could mend his ways and 'turn over a new leaf'.

The High Court substituted the original sentence with one week's imprisonment and a fine of RM3,000, with three months' imprisonment in default, for the first charge and for the second charge, a fine of RM10,000, with one and a half years' imprisonment in default.

SINGAPORE

Title: *Public Prosecutor v Lim Yi Jie* [2019] SGDC 128

Weblink: Weblink (decision not found directly)*

Issue: The accused was involved in a phishing scam but did not execute it directly. The issue was whether they could be convicted under the Corruption, Drug Trafficking and Other Serious Crime (Confiscation of Benefits) Act 1992 for attempting to cash criminal proceeds.

Legislation

- Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (Cap. 65A)

Facts

The accused was involved in a phishing scam, whereby the victim was misled to believe a phishing website was an official bank website, causing the victim to divulge their two-factor authentication details (a time-sensitive PIN number). Although the accused did not execute the phishing scam, which would have been punishable under section 3(1) of the Computer Misuse and Cybersecurity Act, they did attempt to cash two cheques that were criminal proceeds of the scam.

Decision of the court

As the defendant had not executed the phishing scam themselves, they could not be convicted under section 3(1) of the CMCA.

The defendant was convicted under the Corruption, Drug Trafficking and Other Serious crimes (Confiscation of Benefits) Act.

Title: *Re Singapore Health Services Pte Ltd & Ors* [2019] SGPDPC 3

Weblink: Weblink

Issue: Of issue was the cybersecurity practices of health organisations and their failure to put in place reasonable security measures to protect against data breaches.

Legislation

- Personal Data Protection Act (PDPA) 2012, section 24

Facts

A data breach suffered by two health organisations led to a leak of 1.5 million patients' medical records. The Personal Data Protection Commission (PDPC) took enforcement action against: (1) Singapore Health Services Pte Ltd ('SingHealth'); and (2) Integrated Health information Systems Pte Ltd (IHiS) for failing to put in place reasonable security measures to protect personal data under its possession and control. Section 24 of the PDPA requires an organisation to protect the personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the 'Protection Obligation'). The commissioner was satisfied that both SingHealth and IHiS had breached section 24.

Decision of the court

The PDPC imposed a fine of S$250,000 on the first defendant and S$750,000 on the second defendant. The Ministry of Health subsequently issued a Cybersecurity Advisory 1/2019. All licensees (i.e., hospitals, clinics) were strongly encouraged to review the Committee of Inquiry's recommendations and cybersecurity best practices, and to implement relevant measures, where appropriate.

Title: *CLM v CLN and ors* [2022] SGHC 46

Weblink: Weblink

Issue: The plaintiff applied for a freezing injunction against unknown persons, launching a unilateral ex parte lawsuit to reclaim the assets.

Two interesting and novel points of law were raised. First, can stolen cryptocurrency assets be the subject of a proprietary injunction? Second, does the court have jurisdiction to grant interim orders against persons whose identities are presently unknown?

Legislation

The court drew on case law from the UK, Malaysia and New Zealand, as well as the below authorities from Singapore:

- Singapore Civil Procedure 2021 Vol 1 (Cavinder Bull gen. ed.) (Sweet & Maxwell, 2021) ('White Book') at para 81/3/1
- section 18(2) read with para 5(a) of the First Schedule of the Supreme Court of Judicature Act (Cap 322, 2007 rev. ed.)

- *Bouvier, Yves Charles Edgar and another v Accent Delight International Ltd and another appeal* [2015] 5 SLR 558
- *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20

Facts

An American had US$7 million stolen in cryptocurrencies while he was on holiday in Mexico with seven acquaintances, one or more of whom allegedly stole the recovery code to his e-wallet and emptied it within minutes. A portion of the stolen assets, US$1 million was traced to digital wallets at two cryptocurrency exchanges with operations in Singapore. Although digital coins make distribution easier, they also leave a trail that cannot be erased.

Decision of the court

In relation to the first question, the High Court held cryptocurrencies were able to be subject to a proprietary injunction. The court also considered it had jurisdiction to grant ancillary disclosure orders against certain crypto exchanges in aid of the plaintiff's efforts to trace and recover assets. Armed with this order, the plaintiff could attempt to bring actions oversees.

Regarding the second question, the court found that it had jurisdiction to grant interim orders against persons unknown and that it was appropriate to do so in this case, for 9.6 million Singapore dollars (S$) worth of cryptocurrencies. This was the Singapore High Court's first reported freezing injunction against 'persons unknown'.

CASE ANALYSES – CARIBBEAN AND AMERICAS

THE BAHAMAS

Title: *Malik Wright v The Commissioner of Police* [2020] BS CA 45

Weblink: Judgment

Issue: Unauthorised access; revenge porn.

Legislation

- The Penal Code
- The Computer Misuse Act 2003

Facts

The claimant reported the defendant, with whom she had a child, to the police after he took possession of her cell phone during an argument. She was contacted by a friend who informed her that sexually explicit nude photographs of her were circulating on social media. The claimant identified the photographs as ones she had taken of herself and stored as her personal property and did not share them with anyone or authorised anyone to access or publish them. She also noticed that the defendant had made a series of unauthorised transactions on her online bank account. Following the defendant's arrest, IT investigators confiscated a laptop and found that he had downloaded the claimant's data to his laptop, including the claimant's nude photographs and her online banking account information. He was charged with several offences before the magistrates, including fraud by false pretences, contrary to section 348 of the Penal Code ('the PC'), causing damage, contrary to section 328(1) of the PC, and unauthorised access to a computer, contrary to section 3(1) of the Computer Misuse Act 2003. He pleaded guilty to all the charges. Following his sentence, the defendant filed a notice of appeal, stating that the magistrates judge had erred in fact and law as he was never questioned about fraud; failure to notice or take into account the flawed interview and charging process; failed to consider the apparent or actual bias and unfair investigation, which was influenced by the claimant's mother; and for allowing the matters to proceed without inquiring about the irregularity with the prosecution and defence counsel.

Decision of the court

The Court of Appeal upheld the magistrate's decision and precluded the defendant from challenging his conviction. It stated that there was no evidence that the defendant's guilty plea was unequivocal or that it was not made voluntarily. He was fully represented, and his solicitors did not express concern to the court of any impediment that may have hampered their representation of the defendant. The court noted that while the magistrates could have sentenced the defendant to a maximum period of imprisonment of six months pursuant to section 3(1) of the Computer Misuse Act, there was no prospect of success in relation to the defendant's other complaints about his sentence, which required him to serve nine months' imprisonment. As such, he could not use the appeal merely to quash and substitute a lesser sentence on count three.

BELIZE

Title: *Rodolfo Ramos v Simeon Herrera.* Supreme Court of Belize No. 289/2008 [2008]

Weblink: Judgment

Issue: Defamation.

Legislation

- Rule 16.2 of the Supreme Court (Civil Procedure) Rules 2005

Case Law

- *John v MGN Ltd.* 1996 3 WLR 593, at page 607
- *Gleaner Co. Ltd v Abraham* 2003 63 WIR 197 at page 25
- *Sutcliffe e v Pressdram* 1991 1 QB 153
- *RantZen v Mirror Group Newspaper* 1993 4 All ER 975
- *McCarey v Associated Newspaper Ltd No. 2* 1965 2 QB 86 at page 109

Facts

The claimant alleged that the defendant had published defamatory words by sending an email to the claimant's employer to the effect that the claimant had accepted a bribe. The claimant, an architect, knew the defendant, a director of a construction company, through a construction project both had worked on. The defendant's email stated that the claimant had accepted a bribe in exchange for giving the defendant's company a construction contract. The claimant alleged that the email caused him to lose his job, damaged his character and reputation, and that he suffered psychological damage as a result of it.

The claimant brought a claim against the defendant for aggravated and exemplary damages for libel and an injunction to restrain the defendant from publishing the said libel. The defendant failed to file an acknowledgement of service and a judgment in default against the defendant was entered by the registrar. The defendant filed an application to set aside the judgment. The registrar gave leave to the defendant to file a defence. The defendant failed to do so, and a second judgment was entered against the defendant, authorising the claimant to recover damages and granting the injunction.

The claimant applied under Rule 16.2 of the Supreme Court (Civil Procedure) Rules 2005 for an assessment of damages. Both parties submitted affidavits and written submissions to the court.

Decision of the court

The court considered that the libel was published via email rather than a newspaper. It found no evidence that any persons other than the claimant's employer knew the email address or password, or that the libel was published to anyone other than the claimant's employer. The claimant asserted colleagues and former clients became aware of the libel and consequentially stopped doing business with him. The claimant further claimed for loss of income after becoming unemployed and losing the opportunity to earn BZ$5,000 as a sales representative. The court found no evidence that these losses were caused by the publication of the libel. The court noted that the burden of proof of causation was on the claimant to the balance of probabilities. The claimant had not, in the court's view, discharged this burden.

The court did accept that the publication of the libel would have caused psychological pain, suffering, and injured the reputation and character of the claimant in the eyes of his employer. The court awarded compensatory damages for the 'damage to his character and reputation' and for the 'distress, hurt and humiliation which was caused by the libel' [11]. The court noted that when determining the amount of damages, it must 'among other things' 'consider the nature of the libel, the extent to which it blemished the claimant's integrity, reputation and his character and the width or extent of the publication' [11]. The court also considered additional injury, such as the fact that the defendant refused to apologise, as well as: (i) the purchasing power of the dollar, (ii) a comparison with awards in other libel cases, and (iii) a comparison with awards of general damages in personal injury cases.

Damages of BZ$5,000 were awarded as general damages for libel and BZ$2,000 in aggravated damages due to the defendant refusing to apologise, despite having been requested to do so.

CANADA

Title: *Caplan v Atas 2021 ONSC 670*

Weblink: Judgment

Issue: Harassment; defamation.

The court drew on case law from Canada, the UK, New Zealand, as well as Nova Scotia's cyber bullying legislation for support.

Legislation

- Harmful Digital Communications Act 2015 (New Zealand)
- Protection from Harassment Act 1997 (UK)
- The Intimate Images and Cyber-Protection Act, NSN 2017 (Nova Scotia)

Case Law

- *Merrifield v Canada (Attorney General)* 2017 ONSC 1333; 2019 ONCA 205.

Facts

The defendant, who had been a real estate agent in the 1990s, was at the losing end of a mortgage enforcement proceeding and an employment dismissal. After that, she began years-long campaigns to harass her victims using countless internet platforms, sending defamatory emails and letters, alleging they had committed fraud, child exploitation and that they were sexual predators. The accused had been named as defendant in numerous actions brought by the plaintiffs and

had been imprisoned for injunction violations and contempt of court. Despite law enforcement issuing an injunction prohibiting her from posting online comments, she would send malicious messages to their family members and friends, even defaming a victim's deceased spouse.

Decision of the court

Combining four lawsuits together to establish a pattern of harassment against 150 victims, Justice Corbett found that the defendant intended to harass and go beyond character assassination not only on the primary victims, but also on the family and friends of the primary victims. The court in Caplan also held that the existing common law actions were inadequate. The tort required the victim to establish a visible and provable illness and, as such, it would have been unfair to suspend a remedy until a victim fell ill. Defamation was proven, but it was not helpful since the accused was insolvent, making her judgment proof to the remedy of damages. The tort of invasion of privacy was not engaged as the accused modified existing public pictures and did not have any private or personal information about the victims. As such, the court created a new tort of harassment in internet communications to respond adequately to victims. The new tort occurs where the defendant maliciously or recklessly engages in communications conduct so outrageous in character and duration, and extreme in degree, going beyond all possible bounds of decency and tolerance; with the intent to cause fear, anxiety, emotional upset or to impugn the dignity of the plaintiff; and the plaintiff suffers such harm.

Title: *R v Senior 2021 ONSC 2729*

Weblink: Judgment

Issue: Theft; Unauthorised use of a computer database.

Legislation

- Criminal Code (RSC, 1985, c. C-46)

Facts

The accused, a police constable, was arrested following an investigation in which it was uncovered that he inappropriately accessed a police database and shared confidential information, filed an intelligence report about his former mistress, stole a police shotgun and planned to traffic cocaine. He was charged with 14 separate offences including theft under C$5000 (count 1), creating forged documents (counts 2 and 3), unauthorised use of a computer database (counts 4 and 13), breach of trust (counts 5, 10 and 14), possession of a firearm obtained by theft (count 6), possessing a weapon for a dangerous purpose (count 7), attempted robbery (count 8) and trafficking in a Schedule 1 substance (counts 11 and 12).

Decision of the court1

The Ontario Superior Court found the accused guilty of 11 of the charges, while acquitting him on counts 8, 10 and 11. In relation to counts 4 and 13, it found that the defendant's repeated searches of the database were not affected for an official or legitimate purpose relating to the defendant's duties as a police officer and were made for the interest of the defendant and for the purpose of facilitating a criminal offence. He was sentenced to the maximum seven-year sentence.

Title: *R v Usifoh 2017 ONCJ 451*

Weblink: Judgment

Issue: Money laundering; phishing.

Legislation

- Criminal Code (RSC, 1985, c. C-46) Section 380(1)

Facts

The defendant, a Nigerian living in Ontario, was involved in a phishing email scam operating in Nigeria and Dubai and involving fraud totalling over C$200,000. Numerous victims in the United States and elsewhere received emails which contained inheritance scams, romance scams and military scams, trying to lure them to send funds to various accounts belonging to the defendant. He denied knowledge that the funds in his account were obtained by fraud. The issue before the court was whether it could prove beyond a reasonable doubt that the accused knew the funds were fraudulently obtained. It had to be proven that he had actual knowledge or wilful blindness that the funds were fraudulently obtained.

Decision of the court

Rejecting the defendant's evidence, the court held that the claim that he was allowing a 'businessman' to deposit funds into his account so that he was charged less commission on his Western Union

transfer was belied by objective facts. The court noted that while there is no obligation on an accused to call evidence, much of the evidence he provided was contradictory and inconsistent.

Title: *The Brick Warehouse LP v Chubb Insurance Company of Canada*, 2017 ABQB 413

Weblink: Judgment

Issue: Fraud.

Case law

- *Consolidated-Bathurst Export Ltd. v Mutual Boiler and Machinery Insurance Co.*1979 CanLII 10 (SCC), [1980] 1 SCR 888

Additional Resources

- Barbara Billingsley, *General Principles of Canadian Insurance Law*, 2nd ed. (LexisNexis Canada Inc., 2014) at 146

Facts

The applicant, The Brick Warehouse, received a telephone call though to the accounts payable department. The caller claimed to be from Toshiba, and that he was missing some payment details. The Brick employee faxed some payment documentation to the number provided by the caller. The caller repeated the call and story a few days later. This time, The Brick employee advised the caller to write to The Brick's lender to update their contact details to receive electronic payment notifications.

Another employee of The Brick received an email, where the sender claimed to be the controller of Toshiba Canada. The email indicated that Toshiba had changed banks and requested all payments to be made to a new bank account provided. A person called The Brick and spoke with the receiver of the email. They wanted to confirm the change of banking information. After the call, The Brick employee changed the payment details as requested, following standard practice. This paperwork was reviewed by another Brick employee. No one from The Brick took any independent steps to verify the change in bank account or contacted Toshiba to confirm.

A total of C$338,322.22 was paid to the new bank account before the fraud was discovered. An individual claiming to be from Sealy Canada called The Brick, asking for the bank details to be changed to the same new account as Toshiba. The system would not permit duplicate payment accounts. Further, a Toshiba representative called enquiring after missed payments. The Brick reported this to the police and investigations uncovered the fraud. The Brick was able to recover C$113,847.18. The Brick subsequently made a claim to Chubb Insurance for the remaining C$224,475.14. Chubb refused, stating the loss did not fall within the insurance policy.

Decision of the court

The court looked at the insurance policy and its wording. The court followed the two-step interpretation in Consolidated-Bathurst Export Ltd, the first step being to interpret the intention of the parties and the second to resolve any remaining ambiguities. For the first step, the court followed the principles laid down in Barbara Billingsley's leading text on insurance law.

The court held that The Brick's intention was to insure itself against loss arising from criminal action. However, the court maintained that the wording of the policy included the phrase 'without an insured's knowledge or consent'. In this case, the instruction to change the bank details and make the fraudulent payments came from The Brick. The Brick employee gave instructions to the bank to transfer the funds to the new account. Consequently, the court found The Brick did therefore consent to the transfer. The court further noted that even if consent was not found, there was still an issue of whether the transfer was done by a third party. There was no one forcing The Brick employee to make the payment instructions. The court found the transfer was not done by a third party.

The court held that The Brick was not entitled to recover its loss from Chubb.

Title: *R v Martin 2021* NLCA 1

Weblink: Judgment

Issue: Digital evidence.

Legislation

- Section 31.8 of the Canada Evidence Act RSC 1985, c. C-5 [*CEA*]

Case Law

- *R v CB, R v Colosie, R v Farouk*
- *R v Bulldog*

- *R v Hirsch, R v Durocher*
- *R v Richardson*

Facts

Police were dispatched to the residence of the defendant to investigate a complaint of domestic disturbance. When the police entered the home of the defendant and his girlfriend, two other officers had already visited there. They determined that no further investigation into the matter was needed. The following night, police received a tip from an anonymous source that the defendant posted images and words on Facebook that indicated his intentions to harm police officers. Police officers attended the defendant's residence to investigate the threats but were not permitted to enter and were told to leave the property by the defendant. An officer attempted to access the defendant's Facebook, but he was unable to do so. He then contacted the source of the tip and asked that a screenshot of the Facebook posts be emailed to him. Six screenshots of the posts on Facebook were subsequently emailed to the officer. The screenshots depicted the defendant and a masked man holding a gun in different positions, some of which contained threats to the police. During the *voir dire,* which determined whether the screenshots were admissible as evidence and could be used in the trial, several officers who investigated the original complaint were able to identify the defendant and his apartment depicted in the screenshots. The trial judge concluded that the evidence was inadmissible, and the defendant was acquitted.

Decision of the court

The Court of Appeal allowed the appeal. The court stated that Facebook posts fell within the definition of electronic documents, as defined in section 31.8 of the Canada Evidence Act RSC 1985, c. C-5 [*CEA*]. Further, it stated that the proof of authenticity was not held on balance of probabilities, the beyond a reasonable doubt standard nor must the evidence be shown to be capable of determining a finding of authenticity. As per section 31.3, the evidence tendered needed to only be capable of supporting a finding of authenticity. The court also noted that the low threshold for admissibility of authenticated electronic documents had been met, given that the electronic document was what it purported to be.

Title: *R v McNish, 2020 ABCA 249*

Weblink: 2020 ABCA 249 (CanLII) | R v McNish | CanLII

Issue: Breach of trust; Unauthorised use of a computer.

Legislation

- Section 342(1)(c) and Section 122 of the Criminal Code, RSC 1985, c. C-46

Case law

- *R v Braile,* 2018 ABQB 361

Facts

The defendant, a police officer on medical leave at the Calgary Police Service (CPS), was hired by a private security firm to conduct surveillance for a man engaged in a custody battle over his one-year-old child with his common-law partner (the victim). He aimed to collect negative information about the victim for the case and conducted a number of days' surveillance on her, receiving two cheques amounting to 9,000 Canadian dollars (C$). The defendant testified that while engaged in surveillance, he once attempted to replace the battery on the victim's vehicle and even offered to pay her roommate money in exchange for information. He conducted searches on police database on names related to the victim and her roommate. The defendant was convicted for breach of trust under section 122 of the Criminal Code, RSC 1985, c. C-46, and unauthorised use of a computer under section 342.1(1)(c). The defendant made his appeal on four grounds, namely that the trial judge was incorrect in his assessment of his credibility; that he provided insufficient reasons for his conviction for breach of trust under section 122 of the *Criminal Code*; he provided insufficient reasons for his conviction for unauthorised computer use under section 342.1(1) of the *Criminal Code*; and that he should be granted a new trial since his co-accused was successfully granted one.

Decision of the court

Upholding the lower court's decision, the court was satisfied that the trial judge's findings were credible and grounded in the evidence before him. As such, no reversible error had been demonstrated. Second, it found that there had been a breach of trust given that the defendant had used his knowledge of surveillance and tracking devices

obtained through his employment as a police officer to target the victim. He was also not permitted to engage in private security work outside of his employment with CPS. Third, it was clear that the defendant acted without colour of right, as he was not actively involved in his police duties and accessed confidential data for personal use. He did not act honestly and reasonably and could not have held the belief that he was permitted to access the database in the way that he did. His appeal was dismissed.

JAMAICA

Title: *Demetri Hemmings v R (2020) JMCA Crim 44*

Weblink: Judgment

Issue: Possession of Identify Information with intent to use said information to commit an offence.

Legislation

- Law Reform (Fraudulent Transactions) (Special Provisions) Act 2013

Facts

The appellant appealed the decision of the Trelawny Circuit Court, which found him guilty of an offence under section 10(1) of the Law Reform Act 2013 and sentenced him to three years' imprisonment. In the appeal, the appellant's attorney argued that the trial judge reached her decision in the absence of important pieces of information pertaining to the case. At the initial trial, the evidence against the appellant was of emails discovered on his device which, upon examination, indicated a trade in identity information. The digital forensic report submitted as evidence during the trial stated that the email account on the device used to carry out the transaction was in the name of 'dimetrih27' and in some emails the name 'Dimetri Hemmings' appeared beside the email address 'dimetrih27', even though the appellant denied knowledge of the emails and any fraudulent activity.

Decision of the court

The Court of Appeal quashed the conviction of the lower court, set aside the sentence, and entered a judgement and verdict of acquittal for the appellant premised on the evidential oversight of the Crown counsel for failing to disclose and exhibit as evidence the CD where records of transactions and electronic proof of possession of identify information taken from the appellant's iPad was stored.

Title: *Regina v Andrea Gordon [2021] JMSC Crim 6*

Weblink: Judgment

Issue: Money laundering.

Legislation

- Cybercrime Act 2015, Section 4(1)

Facts

The defendant was employed by the National Commercial Bank as a manager at the Operations Branch for almost 30 years. As an employee of the bank, she was issued with a unique access code that she used when undertaking transactions. The manager of the fraud team became suspicious and questioned the defendant about several transactions and withdrawals that were made via her code. The defendant confessed to him that she had misappropriated funds from the bank's internal account. The matter was reported to the police and the defendant was arrested and charged. Following investigations, it was revealed that she had made approximately 282 suspicious transactions totalling J$111,262,660.21 between February 2017 and May 2020. The defendant pleaded guilty to an indictment amounting to J$34 million on 13 counts: three counts of larceny contrary to the Larceny Act; three counts of access with intent to commit an offence to wit, larceny by a servant contrary to the Cybercrime Act 2015; and seven counts of engaging in a transaction that involves criminal property contrary to the Proceeds of Crime Act.

Decision of the court

The defendant was indicted on all 13 counts. The central issue in this case was the defendant's breach of trust when she used the bank's code to access the bank's internal account to remove funds as an employee of the bank. As such, it was held, as per section 4(1) of the Cybercrime Act 2015, she committed an offence because she had access to the bank's internal account and intended to commit an offence.

Title: *Regina v Donovan Powell* (2021) JMCA Crim 11

Weblink: Judgment

Issue: Malicious Communications

Legislation

- The Cybercrime Act 2015

Facts

The victim, DC, and the accused had been involved in an intimate relationship for almost two years. The victim claimed that the accused took nude photographs and videos of her without her permission. After their relationship ended, the victim was threatened that she would be shot, stabbed, ruined or destroyed. The accused sent the victim a video he had created, which contained naked photographs and sexual images, along with vulgar memes and pictures alleging that the victim had a sexually transmitted disease that she had passed on to the accused. A few months later, the accused sent another round of nude photographs and explicit photographs of the victim's genitalia that had been taken when she was sleeping. The accused sent the victim a text message and email with a link to a website that contained the same explicit images and videos of the victim, threatening to inform her friends about the site and send the explicit videos around her son's campus. Following a report to the police by the victim, the accused was subsequently charged and pleaded guilty on three counts of breaches of section 9(1)(a), (b) and (2) of the Cybercrimes Act 2015.

Decision of the court

At first instance, the accused pleaded guilty on all three counts of the Cybercrime Act 2015, as he had used a computer to send obscene data to the victim with the intention to cause harm or to harass her contrary to section 9 of the Cybercrimes Act. He was sentenced to 12 months' imprisonment and ordered to pay a fine of J$1,000,000.00 Jamaican dollars.

The accused subsequently appealed the conviction to the Jamaican Court of Appeal. In deciding to reduce his prison term to six months, the court found that the lower court had erred in its approach to identifying the appropriate starting point for his sentence. Given that the accused was a first-time offender and pleaded guilty on the first occasion, it was found that that he should have his sentence reduced by 50 per cent.

SAINT LUCIA

Title: *Sebastian Marcus Day v The Honourable Attorney General et al.* [2020] SLUHCV2020/301

Weblink: Judgment

Issue: Child pornography.

Legislation

- Computer Misuse Act 2003
- Extradition Act 1994

Facts

The applicant was arrested pursuant to a warrant of arrest issued by the Magistrate's Court. A request for the applicant's extradition was issued to the Government of Saint Lucia by the Government of the United States of America. The basis of the request was a Felony Warrant of Arrest wherein the applicant was charged with 24 counts of possession of 10 or more images of child pornography, imagery, abuse, sexual battery of a child, contrary to Florida statutes 827.071(5) and 775.0847(2) and (3). The judge ordered the applicant to surrender to the United States of America pursuant to the Extradition Act 1994. The applicant appealed his extradition on the grounds that there was no evidence linking him to the pornography, that the offences were not extradition crimes within the meaning of the Extradition Act as pornographic material was not listed in the Act and a crime in accordance with Florida's, and possession of pornographic material was not an offence according to the Computer Misuse Act 2013 as the law only made it an offence to possess pornographic material for the purpose of distribution and facilitating viewership. He also argued that the US Supreme Court in *Stanley v Georgia* (1969) US 557, struck down a legislation which purported to charge an applicant with possession of pornographic material as being unconstitutional and a violation of the first and fourteenth amendments of the United States of America Constitution.

Decision of the court

Dismissing the appeal, the Supreme Court held that the lower court was correct to have found that the offences with which the applicant had been charged were extradition offences. There was sufficient evidence to satisfy the requirements of section 14(1)(b) and (c) of the Computer Misuse Act 2003.The evidence was sufficient to justify the applicant's committal to stand trial for these offences in Saint Lucia. The court also stated that the issues at hand should be dealt with at the trial and not on extradition proceedings. There was also no clear violation of the applicant's constitutional rights, while the court ought not to

entertain argument on the basis of a single case put forward by the applicant. The applicant was surrendered to the requesting state, the United States of America.

TRINIDAD AND TOBAGO

Title: *Therese Ho v Lendl Simmons CV 2014-01949*, (2015) Unreported

Weblink: Judgment

Issue: Revenge porn.

The court drew on case law from the UK, Australia, as well as international human rights conventions.

Legislation

- European Convention on Human Rights and Fundamental Freedoms 1950
- The Human Rights Act, 1998 (UK)

Case Laws

- *Saltman Engineering Co. Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203
- *Coco v AN Clarke (Engineers) Ltd* [1969] RPC41
- *Morison v Moat* 68 ER 492
- *Campbell v MGN* [2004] 2AC457
- *Duchess of Argyll v Duke of Argyll* (1967) 1 Ch 302
- *Wilson v Ferguson* (2015) WASC 15
- *Wainwright v Home Office* [2004] 2 AC406
- *Giller v Procopets* [2004] VSC 113
- *Cornelius v De Taranto* (2001) EMLR 12 at pages 66–67 and 69

Additional Resources

- Gurry on Breach of Confidence: 'The Protection of Confidential Information' 2nd Edition ((p. 107–108)
- Gilbert Kodilinye in: *Commonwealth Caribbean Tort Law* 5th Edition

Facts

The claimant and defendant were involved in an affair. During this time, they both took several nude photographs and sex videos of each other. After their relationship came to an end, the photographs were shown to other people. The claimant subsequently sought an injunction restraining/prohibiting the defendant and others from disseminating, disclosing, using or publishing the nude photographs and videos as this would impede with the claimant's private information and breach her confidence. The claimant also sought an order that the defendant destroy the photographs and other materials, as well as damages for the breach of confidence and aggravated damages.

The plaintiff sued the defendant for breach of confidence, arising from his publishing of intimate photographs of them both to several persons, which subsequently went viral. The defendant was found liable for his breach of the plaintiff's confidence. The judge also cited several English and Australian authorities for the proposition that, although the parties could not claim a right to privacy, the fact of intimacy would be sufficient to give rise to a duty of confidentiality between them. The plaintiff was granted an injunction against further dissemination of the images, damages in the sum of 150,000.00 Trinidad and Tobago dollars (TT$) and costs.

Decision of the court

The claimant's case before the court was founded upon the common law concept of breach of confidence and the court had to consider whether this concept could be applied to the instant facts. Given that there were no local laws that had been developed to recognise the claimant's redress, the court referred to established Australian, English and international conventions on human rights. The judge found that there had been a breach of confidentiality when the photos were distributed, given that the express consent of both parties must be obtained. In terms of the right to privacy, the court could not find an action based on the failure to respect the privacy of a person given that there was no law. The judge emphasised that there was a dire need for the enactment of a statute to afford protection for citizen's person privacy. As the defendant's actions were motivated by a desire to cause the claimant upset, embarrassment and distress, the court held that the claimant was entitled to relief. The claimant was awarded T$150,000.00 in aggravated damages.

CASE ANALYSES – EUROPE

CYPRUS

Title: *Republic v Chatziathanasiou*, Criminal Appeal No. 20/2021, 19/10/2021

Weblink: Judgment of the Supreme Court of Cyprus, Secondary Jurisdiction

Issue: The Attorney-General appealed a sentence of seven years' imprisonment for possession of child pornography, contrary to Articles 8(1)(6) and 14(1)(34) of Law(I)/2014 and possession of pornographic material, contrary to Articles 2, 11(1)(d) and 17 of Law 87(I)/2007.

Legislation

- Law(I)/2014
- Law 87(I)/2007

Facts

The offender was sentenced to five charges of child pornography. Counts one and three concerned pornographic material involving children under 13 years of age. Counts two and four concerned possession of pornographic material involving children over 13 years of age. Count five concerned videos with children's pornographic material of sadistic content with a child under 13 years of age.

Eight hundred and eighty-six (886) files of child pornography were found in the defendant's possession; a significant number involved children under 13 years of age, and many were of the most serious category. The offender was sentenced to seven years' imprisonment. This sentence was appealed by the Attorney-General, who submitted the sentences of three and a half years on counts one and three were manifestly inadequate. The Supreme Court allowed the appeal in part, increasing the sentences on those counts to five years for each, amounting to a total sentence of ten years.

Decision of the court

The judgment made note of the increasing prevalence of online child pornography and the need for strict deterrent penalties. The court considered the seriousness of offending and the long time period over which the offending took place, as well as the offender's remorse, that he did not distribute or create the material, and his blank criminal record.

The court considered the English case of *R v Oliver* [2003] 1 Cr. App. R. 28, which laid down detailed guidelines for child pornography offending, and noted that imprisonment was the only appropriate sentence for this offending.

The court held that the offending was of a particularly serious nature and the long time the offender engaged in the offending was an aggravating factor, as the demand for such materials encourages its creation.

The sentences on counts one and three were increased from three and a half years to five years each. The total sentence therefore increased from seven years' imprisonment to ten years.

Title: *Metaquotes Software Ltd ao v Dababou,* Civil Appeal E324//2016, 14 November 2018

Weblink: Judgment

Issue: Jurisdiction of court; fraud, conspiracy; electronic evidence.

Legislation

- *Norwich Pharmacal Co v Commissioners of Customs & Excise* (1974) AC 133 (EW case)
- *Etc. v Stepanek et al.* (2012) 1 AAD 1403 (CY case)

Facts

The claimant asserted they were victim of a complex fraud and conspiracy by the defendants. The claimants had made investments in the defendant company, with a view to trading in international financial markets using the defendants' technologically innovative programmes and brokerage software. The Supreme Court granted a disclosure order (Norwich Pharmacal order) and appointed an IT expert to obtain and analyse the information stored on complex servers. It was held that the District Court had such jurisdiction to appoint an IT expert and it was justified in this case.

Decision of the court

The Supreme Court upheld the District Court's decision to appoint an IT expert to facilitate the disclosure of electronic evidence. It is likely that the appointment of such independent experts will become more common in complex fraud cases.

MALTA

Title: *Mifsud Av. Cedric Neo v FIMBank PLC* [2020] 501/2020 LM

Weblink: Judgment (in Maltese)

Issue: Hacking; third-party cyberattack.

Facts

Acemar AG was hacked by a third party. The hackers requested FIM Bank to transfer money to a bank account that did not belong to Acemar. FIM Bank did so. In June 2020, the court ordered FIM Bank was to pay a garnishee of $841,941, for its negligence in making the transfer. FIM Bank appealed on the ground that the garnishee was affecting day-to-day operations and its relationship with other banks. The court accepted these arguments in September 2020, ordering the revocation of the garnishee. The court paid regard to the fact that there was no risk to Acemar's credit, and that the presumption should be in favour of the liquidity of the bank.

Decision of the court

The court revoked the garnishee on FIM Bank. Despite alleged negligence in making the payment requested by the hacker, the impact on both the parties, including FIM Bank, was taken into consideration.

UNITED KINGDOM

Title: *R v Akala (Emmanuel)* [2021] EWCA Crim 1994

Issue: The appellant appealed a sentence of 24 months' imprisonment on four counts, to run concurrently. Two of the counts were for securing of unauthorised access to computer material with intent to steal, contrary to section 2 of the Computer Misuse Act, and two were for fraud, contrary to section 1 of the Fraud Act 2006.

Legislation

- Computer Misuse Act 1990
- Fraud Act 2006

Facts

The defendant hacked into Camelot, the National Lottery operator, in an attempt to gain access to personal details of account holders. Six hundred and eighty-four (684) customer accounts were attacked; 160 were successfully accessed, although most not as to receive any sensitive data. The offender was able to access sufficient personal details of 11 customers to get past the security questions on the customer services telephone. The offender called the bank of a Paul Holmes and attempted to transfer £910 to his account but failed. In another attempt, the offender was unable to clear the bank's security questions. There were no direct losses to anyone.

Decision of the court

The offender was originally sentenced to two years immediate custody on each count, concurrent (30 months with a 15 per cent guilty plea reduction and further reduction for the impact of COVID-19 on prisons). The court noted there were no sentencing guidelines for the Computer Misuse Act, emphasising the particular need for deterrence and declining to suspend the sentence. Appeal on that ground was dismissed. The appeal was partially allowed on the ground of the intended loss being so high. Although there were no direct losses, the court assessed the potential loss to be substantial, ranging from £2,500 for the two accounts the offender tried to access, £27,000 for the 11 accounts pursued, £400,000 for the 160 successful log-ins and £1.7million for the 684 attempted log-ins. The judge also considered that the offender would have had appreciation for the positive work Camelot did and reputational damage following the attack.

The case was delayed due to the COVID-19 pandemic. Voice recognition experts were instructed by both prosecution and defence to analyse phone recordings. The evidence served amounted to over 600 pages of witness statements and exhibits. The defendant entered a guilty plea around two months before the trial date, which was listed for seven days. Camelot estimated its costs at £10,000.

The sentence was reduced to 12 months' immediate imprisonment. Counts one and four were reduced to twelve months each and counts two and three were reduced to eight months each, concurrent.

Title: *R v Robins (Samuel John)* [2021] EWCA Crim 848

Issue: Mr Robins sought permission to appeal his sentence of 50 months' imprisonment in total for nine counts of unauthorised access to a computer, contrary to the Computer Misuse Act 1990, section 1, and disclosing private sexual photographs

and film with intent to cause distress, contrary to section 33 of the Criminal Justice and Courts Act 2015.

Legislation

- Computer Misuse Act (CMA) 1990
- Criminal Justice and Courts Act (CJCA) 2015

Facts

The offender hacked into the computers and data of five women, spanning a three-to-four-year period. Some of the victims were known to the offender, two of whom he had been in a relationship with previously, and some were colleagues of his at the Apple Store. The offender was a skilled computer technician. He sought private sexual images from the women's files and posted some online, on social media and revenge porn sites, sometimes with the victims' personal details. Many of the victims received unwanted and abusive contact from strangers as a result. The offender also sent links to the sites to some of the victims and people they knew, including one of their bosses. Images were found stored on the defendant's hard drive. The offender pleaded guilty to nine counts.

- Counts one and three: posting explicit images of victim 1 (V1) on at least three websites. CMA 1990, section 1: four months' imprisonment. CJCA 2015, section 33: six months' imprisonment, concurrent.
- Count four: posting images of V2 on social media and a revenge porn website with their personal details. V2 had known the offender for many years. CMA 1990, section 1: ten months' imprisonment, consecutive.
- Counts five and six: posting images of V3 online, linked to her Facebook account. The offender had worked with V3 at the Apple Store. CMA 1990, section 1: six months' imprisonment. CJCA 2015, section 33: ten months' imprisonment, concurrent, to run consecutively to the others.
- Counts seven and eight, and nine and ten: images of V4 and V5 were posted online. Fifty-seven (57) images of V4 were found on the offender's hard drive. The offender had gained access to their computers in 2013–14 when he repaired them. CMA 1990, section 1: six months' imprisonment. CJCA 2015, section 33: ten months' imprisonment, concurrent, to run consecutively to the others.

Decision of the court

The Court of Appeal dismissed the appeal.

The court referred to the sentencing judge's remarks that 'there were no guidelines for the Computer Misuse Act offences' [para 10]. Reference was made to *R v Martin* [2013] EWCA Crim 1420, and that 'the sentence should reflect the sophistication, the sensitivity of the data, the repeat nature and the breach of trust' [para 10].

The grounds of appeal were that insufficient regard was given to personal mitigation and the principle of totality. The personal mitigation focused on the applicant's partner struggling to cope alone as a single parent, with difficulty accessing state benefits as a foreign national. For totality, the submission was simply that the sentence was too high. The applicant conceded the offending was appalling and that the judge was not faced with a straightforward sentencing exercise.

The court noted the offending was lengthy and sophisticated, involving five separate victims, with obvious distressful consequences. The court held the 'offences were very serious examples of their type'. Despite some temporal overlap in the offending, the consecutive sentences were upheld.

Title: *R v Mudd (Adam Lewis)* [2018] 1 Cr. App. R. (S.) 7

Weblink: CPS Guidance Example

Issue: The offender appealed his sentence of two years' detention for unauthorised acts with intent to impair the operation of computers, contrary to the Computer Misuse Act 1990, section 3(1) and section 6, making, supplying and offering to supply an article for use in an offence, contrary to the CMA 1990, section 1 and section 3, and concealing criminal property, contrary to the Proceeds of Crime Act 2003, section 327(1).

Legislation

- Computer Misuse Act 1990
- Proceeds of Crime Act 2003

Facts

The offender, when he was 16, created a computer program designed to carry out 'denial of service (DoS)' attacks on websites. Over a period of 18 months, he carried out some attacks, but primarily provided the program to others. Although he had not been motivated by financial gain, he had run the program 'for hire'. He had 112,298 customers and received around £248,000 through numerous false PayPal accounts that the defendant had created using false details. The program was used to carry out 1.7 million attacks on websites worldwide, on 666,532 internet protocol (IP) addresses or domain names.

The offender pleaded guilty to three counts and was sentenced to two years', nine months' and two years' detention, concurrent, in a young offender institution. The sentencing judge held that had he been an adult, he would have been sentenced to six years' imprisonment, given the very high level of culpability. The judge reduced that to 32 months to take account of his youth and medical condition and gave a 25 per cent credit for the guilty plea. Two years' immediate detention was ordered at first sentencing.

Decision of the court

The offender appealed on the grounds that his age and vulnerability meant that the sentence should have been suspended. The offender had autistic spectrum disorder and his offending had been about meeting his emotional and social needs. The pre-sentence report (PSR) indicated low-risk of further offending and that the defendant was vulnerable and would find custody very difficult. The PSR recommended a community-based sentence.

On appeal, it was noted that there were no sentencing guidelines for the CMA 1990 and that it was necessary to have regard to culpability, harm, deterrence and punishment. The court had to send a clear message that such cybercrime would be taken very seriously and punished accordingly. The Appeal Court held the sentencing judge had paid regard to all the circumstances and had not erred in imposing an immediate custodial sentence.

On the reduction for guilty plea, the Appeal Court held the full one-third reduction should have been reserved. Counsel was ill at the plea before venue hearing and a colleague had stepped in; a disk was presented by the prosecution, to which counsel asked for time to consider. The offender's age and vulnerability meant he was unlikely to overrule counsel's advice. These were exceptional circumstances. The 24-month sentence was quashed and replaced with one of 21 months' detention.

Title: *R v Svetoslav Donchev* [2020] EWCA Crim 477

Issue: The offender appealed a sentence of nine years' imprisonment for making articles for use in frauds, contrary to section 7(1) of the Fraud Act (FA) 2006; supplying articles for use in frauds, contrary to section 7(1) of the FA 2006; encouraging or assisting the commission of one or more offences, contrary to section 46 of the Serious Crime Act (SCA) 2007; concealing, disguising, converting, transferring criminal property, contrary to section 327(1) and section 334 of the Proceeds of Crime Act (PCA) 2002; and acquiring or possessing criminal property, contrary to section 329(1) of the PCA 2002.

Legislation

- Fraud Act 2006
- Serious Crime Act 2007
- Proceeds of Crime Act 2002

Facts

The offender was extradited from Bulgaria for his role in writing and distributing complex malware packages and marketing them to fraudsters internationally. He created website scripts for up to 53 UK-based companies, or companies with a UK footprint. It was estimated that there were potentially half a million victims as a result of his criminal activity, with the fraud totalling £41.6 million.

The offender was sentenced on five counts to a total of 9 years imprisonment.

- Counts one and two: FA 2006, section 7(1): five years' and three months' imprisonment, concurrent.
- Count three: SCA 2007, section 46: six years' and nine months' imprisonment, concurrent to counts one and two.
- Count four: PCA 2002, section 327(1) and section 334: two years' and three months' imprisonment, consecutive to counts one to three.

- Count five: PCA 2002, section 329(1): 18 months' imprisonment, concurrent to count four.

Decision of the court

The Appeal Court upheld the sentence and dismissed the appeal. It considered it 'wrong to focus on gain in offending of this particular nature where the actual or potential losses are vast'.

Title: *Tuckers Solicitors LLP; Monetary Penalty Notice from the Information Commissioners Office (ICO),* 28 February 2022

Weblink: ICO Order

Issue: Breach of data protection regulation following a cyberattack, for failure to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, contrary to Article 5(1)(f) of the General Data Protection Regulation (GDPR), and failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including: (a) encryption, and (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, contrary to Article 32(1)(b) of the GDPR.

Legislation

- General Data Protection Regulation
- Data Protection Act 2018

Facts

In August 2020, Tuckers Solicitors suffered a ransomware attack that encrypted 972,191 files and released some stolen data onto the Dark Web. Despite accepting the attackers were primarily culpable, the Information Commissioners Office (ICO) found Tuckers had breached Articles 5(1)(f) and 32(a)(b) by failing to implement appropriate security measures. The breach involved court files, including personal and sensitive data. The ICO pointed to Tuckers' failure to implement multi-factor authentication, a security patch and encryption, noting the relative low cost of these measures in comparison to the risks of a breach when determining whether Tuckers had been negligent.

Decision of the court

Tuckers was fined £98,000. Consideration was given to Tuckers financial position and the nature of the work undertaken by the firm.

Title: *R v Steffan Needham* [2019] EWCA Crim 1541

Weblink: Court Transcript

Issue: Computer misuse; unauthorised access; unauthorised modification.

Legislation

- Section 1 and 3 of the Computer Misuse Act 1990

Facts

The defendant, an IT consultant, was employed on a four-week contract for a company that provided cloud-based online services. The company had customers in the United Kingdom and Australia and used servers provided by Amazon Web Services (AWS) for storage of information for their customers. During the course of the contract, the company did not think that the appellant had the required skilled set and decided not to renew his contract. After the defendant was terminated from employment, he accessed his employer's system, using a username 'Speedy', and terminated 23 of his former employer's servers. An investigation of the IP address that deleted the servers was traced to the appellant and he was arrested. The case went to trial, and he was charged with unauthorised access to computer material, contrary section 1 of the Computer Misuse Act 1990 (count one), and unauthorised modification of computer material, contrary to section 3 of the Computer Misuse Act 1990 (count two). It was estimated that the termination caused significant financial damage to his former employer, in the region on £500,000. Nine employees were also made redundant as a result of the appellant's conduct. He was sentenced to two years' imprisonment.

Decision of the court

The court dismissed the appeal and upheld the lower court's decision. While the appellant claimed that the removal of servers from his former employer was accidental, the judge did not accept this explanation given that the appellant had changed the password for the username before using it to delete the servers. Furthermore, it was clear to the judge that the appellant harboured a grudge due to not having his contract renewed and revenge was an aggravating factor. There had been an element of planning as the appellant had 24 hours to reflect and was not deterred.

Title: *PML v Person(s) Unknown (responsible for demanding money from the claimant on 27 February 2018)* [2018] EWHC 838 (QB)

Weblink: Judgment

Issue: Cyberattack; blackmail.

Legislation

- Section 12 of the Human Rights Act 1998

Facts

The claimant company suffered a cyber hack of its computer system, leading to a very large quantity of data being stolen. The defendant sent an email to three directors of the claimant threatening to publish the stolen data unless a ransom of £300,000 was paid in Bitcoin in two weeks. Email communication between the claimant and defendant continued. The claimant had no intention of paying the sum demanded, but kept the defendant engaged to buy time. The claimant immediately reported the matter to the police.

The claimant applied to the court, without notice, for an 'interim non-disclosure order to restrain the threatened breach of confidence and for delivery-up and/or destruction of the stolen data' [5]. Bryan J sat in private and granted the injunction with a series of further orders, including anonymising the claimant and restricting access to the court file (the 'injunction order'). Bryan J was satisfied that the conditions of section 12(3) and section 12(2) of the Human Rights Act 1998 were satisfied, respectively, that the claimant was likely to demonstrate at trial that publication of the stolen documents would not be allowed, and that the claimant appeared to be a victim of blackmail created a risk that, were the defendant given notice of the application, they would publish it.

The information was published online by the defendant. The claimant obtained an order from a court in the European jurisdiction of the website server to block access to the site, which was done. Further postings were found on various forums and websites. the hosting companies blocked access to the sites following the injunction order.

The claimant initiated proceedings against the defendant. They further issued an application notice seeking the continuation of the injunction order before trial.

Decision of the court

The court granted the continuation of the injunction order. The court considered that little had changed since the order was granted. The court was satisfied that there was a continuing threat to publish the stolen documents in breach of confidence. The court was satisfied that the conditions of section 12(2) and (3) continued to be met. The defendant had not suggested there was any public interest that could justify publication. The defendant had breached the injunction order by failing to deliver up or delete the stolen data; this, in the court's view, justified its continuation.

The court was satisfied to hear the application in private pursuant to Civil Procedure Rules (CPR) Part 39.3(a)(c)(g), finding powerful evidence that the defendant was blackmailing the claimant and that the purpose of the proceedings would have been frustrated if heard in public. The court was further satisfied to continue the anonymity of the claimant and restrict access to certain court file documents so as to not defeat the order.

In addition, the court made an order requiring the defendant to self-identify. The punishment for contempt of court thus loomed if the defendant defied this order.

The court noted that the defendant may be resident in a country outside England or Wales, requiring the court's permission to serve the claim form outside the court's jurisdiction. The court considered that the threatened act (publication) and detriment suffered would be within the jurisdiction. The court granted permission under CPR Part 6.37 and Part 6 PD6B §3.1(21) to serve documents out of jurisdiction, as required. The court required the claimant to take steps to conclude the action in the event that the defendant did not file a defence, either by applying for default and/or summary judgment by 23 May 2018.

CASE ANALYSES – PACIFIC

AUSTRALIA

Title: *X v Twitter Inc [2017] NSWSC 1300*

Weblink: Judgment

Issue: Should the court grant ex parte injunctive relief against foreign defendants? What is the effectiveness of worldwide takedown orders?

Legislation

The case drew on Australian and UK case law:

- *Streetscape Projects (Australia) Pty Ltd v City of Sydney* [2013] NSWCA 2
- *X v Y & Z* [2017] NSWSC 1214 at [20]
- *Macquarie Bank v Berg* [1999] NSWSC 526
- *Maggbury Pty Limited v Hafele Aust Pty Limited* (2001) 210 CLR 181

Facts

In 2017, a fake Twitter handle adopting the name of the claimant CEO and disclosed confidential information about him. The claimant asked Twitter to remove the material from its website, along with a request to deactivate the user's account so no further confidential information and disclosure of identity and contact information of the user's identity could be published. Twitter removed the account. However, weeks later a separate account appeared, following the same pattern as before. Twitter subsequently permanently suspended the user's account. The tweets continued to appear weeks later and 11 tweets from an account named after a provocative descriptive noun appeared, which were indicative of the nature of the conduct being undertaken. This time Twitter refused to take down the content and argued that there was no impersonation and that it did not violate its terms of service. Many bold and threatening tweets appeared again, and Twitter refused to take them down for similar reasons as before.

Decision of the court

The court concluded that that the user had breached its contractual obligations of confidence to X. Twitter's refusal to remove the tweets was contrary to Twitter's rules (that it would not publish or post its users' private and confidential information without their permission). The court held that Twitter owed X an equitable obligation of confidence, as it had been told of the confidential nature of information and the way in which it was unlawfully obtained. The court rejected Twitter's argument that the court could only restrain a party to comply with laws of New South Wales (NSW) and restraint of publication of material outside NSW exceeded its limits and powers. Twitter decided not to participate in the proceedings or to submit to the jurisdiction of the court.

Furthermore, the court rejected Twitter's argument that the Supreme Court could only restrain a party to comply with laws of New South Wales and that it exceeded its limits and powers. It concluded that the court had acquired jurisdiction for a foreign defendant because the injunction had a proscribed connection to the case. The injunction was sought by X to compel or restrain the conducts everywhere in the world, including Australia.

Regarding discretion, the court was satisfied that its orders should achieve the minimum necessary and not be exorbitant. It decided to exercise its discretion because the tweets contained commercially sensitive confidential information; X's confidential information was published with their consent; X did not know the identity of the user and could not restrain them from further publication; Twitter had the user's name and contact details; and if the user was not restrained from further publishing X's confidential information, there was a foreseeable risk that X may suffer irreparable damage.

The court decided that it was important to make the order given the size, popularity and social responsibility of Twitter, even though it could not ensure Twitter would comply with orders made in a foreign jurisdiction.

Title: *Martin v Henderson* [2020] WASC 473

Weblink: Judgment

Issue: Harassment.

Legislation

- Section 20 Crimes Act 1914
- Section 5.6 and Section 474.17 Criminal Code Act 1995

Facts

It was alleged that the appellant had sent a series of text messages by telephone to his son-in-law. The defendant was convicted in the Magistrates Court on two charges that he used a carriage service in such a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive contrary to the Criminal Code Act 1995. On conviction, an order was made under section 20(1)(a) of the Crimes Act 1914, which required the defendant to be of good behaviour for six months, on a bond of $1,000. The defendant appealed both the conviction and sentence, stating that he did not have access to the relevant phone number at the time of alleged offending, that the magistrate refused to take evidence from his wife, the magistrate exhibited bias, his computer was interfered with and that his legal representation was inadequate.

Decision of the court

Dismissing the appeal, the court found that the grounds of appeal had no merit.

Title: *R v Schipanski* [2015] NSWDC 381

Weblink: Judgment

Issue: Child pornography.

Legislation

- Section 91H(2) Crimes Act NSW
- Section 474.19(1)(a)(i) of the Commonwealth Criminal Code

Facts

It was alleged that the defendant used the internet to access online child exploitation material. In 2011, he became known to law enforcement due to an investigation by the police which identified his internet protocol (IP) address as being subscribed to a child exploitation material share folder as part of a peer-to-peer program. He was also the subject of another investigation that connected his IP address with a child exploitation material share folder in 2013. Following this two-year investigation, the police executed a search warrant of his property, whereby the police found child exploitation material on various USBs, disks and computers. It was calculated that he was in possession of approximately 20,000 images and 2,000 videos containing child exploitation material. The defendant was arrested and charged with four offences, including using a carriage service to access child exploitation material contrary to section 474.19(1)(a)(i) of the Commonwealth Criminal Code. The other three charges were possession of child abuse material contrary to section 91H(2) Crimes Act 1900 (NSW) arising from the CDs and hard drives where the data was located.

Decision of the court

The defendant pleaded guilty to all four offences alleging access to and possession of child exploitation material. Prior to his arrest, the defendant was suffering from post-traumatic stress disorder (PTSD), depression, anxiety and stress, and this was taken into account in sentencing. He was sentenced to a minimum term of imprisonment of one year and three months, upon which he was to be released upon entering a recognisance pursuant to section 20(1)(b) in the sum of A$200 to be of good behaviour for a period of one year and six months under supervision. His USB, CDs and DVDs were also forfeited to the Commonwealth.

Title: *R v Whittaker* [2021] ACTSC 189

Weblink: Judgment

Issue: Child pornography.

Legislation

- Crimes Act 1900 (ACT) sections 55, 56, 61, 64, 65
- Crimes Act 1914 (Cth) sections 16A, 16AAB, 16AAC, 19, 19AB, 19AF, 19AJ
- Crimes (Sentencing) Act 2005 (ACT) section 7, 14, 33, 35
- Criminal Code Act 1995 (Cth) sections 473.1, 474.22A, 474.27A, 474.29AA
- Firearms Act 1996 (ACT) s 181

Facts

The claimant was employed at a supermarket when she was 14 years old, and the defendant was a manager at the time of the offences in 2017. He was not the claimant's supervisor, but his duties gave him access to the supermarket's rostering system, which contained the personal information of each employee, including their date of birth. The defendant and the claimant began to communicate on New Year's Day in 2018 using Snapchat, where the defendant sent messages to the claimant that

she was perfect, beautiful, and that he loved and cherished her. He again messaged her on her 15th birthday and on Valentine's Day. The claimant and defendant used Snapchat to communicate almost daily, with some messages that were overtly sexual in nature. Between 2018 and 2019, their relationship involved sexual activity, including penile/vaginal intercourse, fellatio and other sexual acts. In 2019, the police and authorities in other countries received a referral from New Zealand concerning a Mega.nz account that was linked to a Hotmail email address in the defendant's name. The account was created in 2016 and stored files that were deemed child abuse material within section 473.1 of the Criminal Code 1995. The police executed a search warrant of the defendant's work premises and from here he accompanied police officers to his home. During the search, police found a computer and two phones that contained video files depicting children between the ages of 18 months and 12 years old in sexual poses, in sexualised poses and subjected to acts of indecency. He was arrested and charged on 25 counts, including using a carriage service to transmit an indecent communication to a person under 16 years of age, contrary to section 474.27A(1) of the Criminal Code Act 1997, and possessing child abuse material obtained by using a carriage service, contrary to section 474.22A(1) of the Criminal Code Act 1995.

Decision of the court

The court found the defendant guilty on all 25 counts. By virtue of the claimant's age, the court found that she lacked the capacity to give real consent. The relationship was said to be inherently abusive and caused significant harm to the claimant. In relation to each charge, the offender pleaded guilty in the Magistrates Court and, pursuant to section 35 of the Crimes (Sentencing) Act 2005 (ACT) (Sentencing Act), the sentences were discounted by 25 per cent. He was sentenced to nine years and six months' imprisonment.

FIJI

Title: *State v Hannan Wang, Guangwu Wang & Xuhuan Yang* [2019]

Weblink: Judgment

Issue: Money laundering.

Legislation

- Section 69(2)(a) and 3(b) Proceeds of Crimes Act 1997

Facts

It was alleged that the three defendants colluded to launder money into accounts through their companies. Investigations by the bank revealed multiple repetitive transactions from foreign cards that could not be supported by receipts or proper transaction details and were deemed suspicious. Two of the defendants, Hannan Wang and Guangwu Wang, were charged with two counts of money laundering in the Magistrates Courts, contrary to section 69(2)(a) and 3(b) of the Proceeds of Crimes Act 1997. The third defendant, Xuhuan Yang, was charged with one count of money laundering, contrary to section 69(2)(a) and 3(b) of the Proceeds of Crimes Act. It was alleged that the first two defendants engaged in money laundering to the sum $687,109.14 between 9 and 24 June 2015. It was also alleged that Yang engaged in laundering money to a total sum of $8500 on 18 June 2015. The defendants appealed the decision to the High Court in Fiji at Suva.

Decision of the court

While the court was satisfied beyond a reasonable doubt that the monies contained in the count at the time of the withdrawals were proceeds of crime within the meaning of section 3 and section 4(IA) of the Proceeds of Crime Act 1997, it was not, however, satisfied that the defendants knew or ought to have known that the monies they were withdrawing had come from unlawful activity. Moreover, there was no evidence that they were involved in opening the two bank accounts with the bank. As such, they were acquitted on money laundering charges.

Title: *Fashion Week v Emosi Radrodro [2017]*

Weblink: Link

Issue: Cyber defamation.

Legislation

The case relied on UK and Canadian case law.

- *Al Amoudhi v Brisard and Another* [2007] I WLR 113
- *Capital & Counties Bank v George Henry & Sons* [1881] 7 App Cases 741
- *Pritchard v Van Nes* [2016] BCSC 686
- *Lewis v Daily Telegraph Ltd* 1964 AC 234

Facts

Radio personality, Emosi Radrodro, published a series of defamatory and false statements on Facebook about Fiji Fashion Week (FFW) and its managing director. The plaintiffs sought damages and claimed that the comments were made with intent and malice to cause injury to them. The plaintiffs claimed that their reputation had been seriously damaged, and their business suffered losses and damage.

Decision of the court

The High Court ruled that comments made by the defendant directed at the managing director (Mrs Whippy-Knight) were defamatory and libellous. The court ordered him to pay $10,000 to Mrs Whippy-Knight, in addition to costs summarily assessed in a sum of $2500. Regarding Fiji Fashion Week, the court found that comments made by defendant to FFW were neither defamatory nor libellous. As such, they were ordered to pay the defendant $2000 in court costs for bringing the action. The court also rejected the defendant's claim that it was someone else who published the statements on Facebook and it did not absolve him of his responsibility towards the comments that he made, which were widely circulated.

Title: *State v Naidu et al. [2018] FJHC 873; HAC59.2013 (18 September 2018)*

Weblink: Judgment

Issue: Whether the defendants engaged directly or indirectly in transactions that were the proceeds of crime knowingly or ought to have reasonably known that the money was derived from some form of criminal activity.

Legislation

- Section 69(2)(a) and (3)(a) of the Proceeds of Crime Act 1997

Facts

Three defendants were accused of hacking into the electronic banking facility of several accounts of a bank and making unauthorised online transfers into two other accounts. The stolen money deposited in these accounts was later withdrawn on the instructions of the first defendant. The second defendant gave the withdrawn sums to the first defendant, who then transferred the money to Nigeria through Western Union. He was helped by the third defendant, who was a teller at Western Union. Following investigations, the three were arrested and charged with the following offences: the first defendant was charged with four counts of money laundering contrary to Section 69(2)(a) and (3)(a) of the Proceeds of Crime Act 1997; while the second and third defendants were charged with one count of money laundering contrary to Section 69(2)(a) and (3)(a) of the Proceeds of Crime Act 1997.

Decision of the court

The court found the three defendants guilty on all six counts. They had engaged directly or indirectly in transactions that were the proceeds of crime knowingly or ought to have reasonably known that the money was derived from some form of criminal activity. In the case of the first defendant, the court noted that he was the main culprit and had co-ordinated the entire criminal enterprise. He used sophisticated methods and involved innocent people in his crimes. He was sentenced to six years and nine months' imprisonment and was ordered to pay a restitution of FJ$12,000 to the bank within a year. The second defendant was sentenced to three years' imprisonment and a non-parole period of two years, given that she was an innocent participant and scapegoat. The third defendant was sentenced to six-and-a-half years' imprisonment, given that she had assisted the first defendant and had breached the trust of the employer and failed to follow the guidelines and protocols of the bank.

NEW ZEALAND

Title: *Kim Dotcom, Finn Batato, Mathias Ortman & Bram Van Der Kolk v United Sates of America & District Court of North Shore SC 30/2013 [2014] NZSC 24*

Weblink: Judgment

Issue: Enforcement of extradition orders under section 2 of the New Zealand Extradition Act 1999, for charges of cybercrimes (money laundering, racketeering and wire fraud).

Legislation

- New Zealand Extradition Act 1999

Facts

The minister of justice had applied for extradition of the appellants to the United States on criminal charges of copyright infringement, money laundering, racketeering and wire fraud arising

out of the operations of the Megaupload group of companies, which provided storage of electronic files. These storage sites are said to have been used for massive sharing of files, in evasion of copyright. An appeal of an interlocutory order thus concerned disclosure of documents relied on to establish eligibility for surrender under Part 3 of the Extradition Act 1999.

The appellant eligibility for surrender was established under section 24, if a judge of the District Court was satisfied that the evidence given or produced would justify the person's trial in New Zealand and that no restrictions on surrender applied. The determination was made at a hearing conducted on the same basis as a committal hearing for an offence committed in New Zealand. Although the final decision whether to surrender someone found to be eligible is a government decision, the question of eligibility for surrender is determined by judicial process and according to New Zealand law, as is made clear by both the Act and the extradition treaty between New Zealand and the requesting country, in this case, the United States of America.

The Court of Appeal had overturned orders for disclosure first made in the District Court and upheld on judicial review to the High Court. It held that section 25 did not require provision of copies of the documents relied on to establish a prima facie case if their effect was summarised in the summary of evidence in the record of the case. It held also that the court may require disclosure of documents not included in the record of the case only where necessary 'to protect the integrity of its processes'.

The court accepted that someone resisting a prima facie case might be:

. *able to point to gaps or flaws in the material summarised or analysed in the record of the case, or to point to documentary or other evidence which causes the extradition court to doubt the reliability of the material proffered by the requesting state*

And to conclude that a prima facie case was not established. But it considered that:

. *a challenge which did not go to the reliability of the material in the record but to its interpretation, that is, to the inferences that should be taken from it, was more appropriate to a trial than to an extradition hearing.*

Because of this analysis of the limited functions of the extraditing court, the court of Appeal concluded that the disclosure orders in the case had been wrongly made.

Decision of the court

The Supreme Court, in a majority decision (McGrath, William Young and Blanchard JJ) dismissed the appeal. It was determined that there is no right of general disclosure in extradition proceedings; requesting states can, subject to the duty of candour, decide what material to put before the court deciding on eligibility to surrender; under the duty of candour, requesting states must disclose any evidence that would render worthless, undermine or seriously detract from the evidence upon which they rely, whether on its own or in combination with material that is in the requesting state's possession or is drawn to its attention by the requested person or the court; and the New Zealand authorities assisting or acting on behalf of requesting states must stress the importance of that duty to requesting states and use their best endeavours to see that it is complied with. It was therefore concluded that nothing had been put forward to suggest that the appellants needed any further material in order to have a fair hearing.

Dissenting, Judge Elias CJ disagreed with the Court of Appeal on both conclusions. It was determined that considering that section 25(2) of the Extradition Act required the provision to the person against whom extradition was sought of the documents relied upon to establish a prima facie case justifying trial and therefore extradition, since the Court of Appeal accepted that the record of the case on this view was incomplete, the deficiency must be remedied if the minister wished to proceed on it. He determined that the disclosure ordered in this case went no further than the disclosure necessary to inform those who were the subject of the hearing of the prima facie case against them. The Supreme Court allowed the appeal from the Court of Appeal and substantially reinstated the orders made in the District Court.

Title: *R v Black (2022) ACTSC 4*

Weblink: Judgment

Issue: Stalking; use of carriage service to menace, harass or cause offence.

Legislation

- Crimes (Sentencing) Act 2005
- Crimes Act 1900
- Crimes Act 1914 (Cth)
- Criminal Code Act 1995

Facts

Mr Steven Black, the offender, pleaded guilty to three counts of offences of use of a carriage service to menace, harass or cause offence, contrary to section 474.17(1) of the Criminal Code Act 1995 (Cth) (Criminal Code). The first offence occurred between 18 April and 31 July 2020, where the offender called his first accuser Ms Natalie Foster (a pseudonym) 117 times. These calls were made without Ms Foster's permission using a private number and were hung up before they could be answered. It is worth noting that the offender called Ms Foster 117 times on a particular day and 17 times on another day. The second offence happened between 27 June and 31 July 2020, when the offender made several social media posts about Ms Foster and sent her numerous requests on Twitter accounts via fake accounts. The third offence occurred between 7 July and 31 July 2020, where the offender communicated with and about the second accuser, Ms Cooping (a pseudonym), via social media. He made several posts on Facebook that related to Ms Cooper and sent her a follow request on social media using a pseudonym account. Even though the posts on social media did not explicitly name Ms Copper, they were – like the ones about Ms Foster – symbolic, suggestive and cryptic. Ms Cooper reported the follow request to the police and the posts she saw on the offender's social media page, which appeared to be about herself and Ms Foster.

Decision of the court

The offender in his defence attributed his offending to mental health illness, claiming that due to his mental condition, he believed that Ms Foster wanted to speak to him – hence the persistent calls. The defence team successfully established that the offender was suffering from delusional disorder, a severe mental disorder within the schizophrenia spectrum.

In recognition of the significant impact that the actions of the offender had had on Ms Foster and Ms Copper's well-being, plus Mr Black's mental health condition, the court sentenced him to 18 months' imprisonment for the first offence, reduced to 13-and-a-half months on account of his guilty plea. On the second offence, he was sentenced to 18 months' imprisonment, reduced to 13-and-a-half months on account of his guilty plea; and on the third offence, he was also sentenced to 18 months' imprisonment, reduced to 13-and-a-half months on account of his guilty plea. The sentences were partly concurrent and partly cumulative, and the court held that the sentences of imprisonment were to be served by way of an intensive correction order (ICO) pursuant to section 11(3) of the Sentencing Act for a period of three years.

Title: *R v Iyer [2016] NZDC 23957*

Weblink: Judgment

Issue: Whether the defendant was guilty of breaching a protection order contrary to section 49(1)(b) of the Domestic Violence Act 1995 and breach of section 22 of the Harmful Digital Communications Act 2015

Legislation

- Section 49(1)(b) of the Domestic Violence Act 1995
- Harmful Digital Communications Act 2015 (HDCA)

Facts

The defendant (husband) and claimant (the wife) were married but separated at the time of offending. The defendant told the claimant that he accessed her Google Maps account on her smartphone and used it to track and follower her while she was in the company of another man. A few days later, the defendant threatened to post pictures of his wife online. Pictures of the claimant were posted on Facebook of her lying on a bed in her underwear. The respondent contacted Facebook and made a police complaint. The defendant admitted to the police that he created an account and uploaded two photographs to it. The defendant was charged with two offences. The first was breaching a protection order, contrary to section 49(1)(b) of the Domestic Violence Act 1995. The second charge alleged a breach of section 22 of the Harmful Digital Communications Act 2015 (HDCA). It was alleged the defendant posted a digital communication of semi-nude

images of his ex-wife. The prosecution alleged that when the defendant posted the communication, he intended to cause the claimant harm; that posting the communication would cause harm to an ordinary reasonable person in the claimant's position; and that posting the communication caused serious emotional distress to the claimant.

Decision of the court

The application in respect to the first charge (breach of a protection order) was dismissed. In order to find the defendant guilty of the second charge (breach of section 22 of the Harmful Digital Communications Act 2015), the prosecution had to satisfy five elements, namely: (a) the defendant posted a digital communication; (b) on or about 29 August 2015; (c) with intention to cause harm to the claimant; (d) posting the communication would cause harm to an ordinary reasonable person in her position; and (e) posting the photographs did cause harm, being serious emotional distress, to the defendant. While the prosecution was able to establish the first four elements, they failed to cross the threshold in respect of element five of the second charge (section 22 HCDA). The court argued that it was not enough to prove that the digital communication would cause harm to an objective person. The prosecution failed to establish that the communication caused harm to the victim. Emotional distress was not sufficient to satisfy the court that it reached the threshold of serious emotional distress. As such, the application was dismissed.

Title: *New Zealand Police v B* [2017] NZHC 526

Weblink: Judgment

Issue: Whether the judge erred in his decision by: (1) applying language other than the statutory language in relation to serious emotional distress; and (2) concluding the evidence could not establish that distress.

Legislation

- Harmful Digital Communications Act 2015
- The New Zealand Bill of Rights Act 1990

Facts

The respondent and claimant separated, and she obtained a temporary protection order against the defendant. A few months later, the claimant went out with another man. The following day, the defendant sent the man a text message and asked him if he had fun with 'my wife'. The claimant called the defendant. He described the car she was in, the man she was with and his address. He also stated that he was waiting outside the man's home and then left. The defendant and claimant met later that month at a park where the defendant told her that he had lots of photographs of her and that he would post them online if she did not stay away from other men. He also told her to cancel the protection order. A friend of the claimant (J) had a new follower on Facebook. J clicked on the profile and saw nude pictures of the claimant. The claimant contacted Facebook and then made a police complaint. The defendant was charged with breaching a protection order in relation to his estranged wife and causing her harm through posting a digital communication contrary to the Harmful Digital Communications Act (HDCA) 2015. The judge in the lower court found the first charge proved, but concluded the second charge could not be found as the evidence was incapable of establishing the defendant had caused the claimant 'harm', defined as 'serious emotional distress'. He concluded that evidence could not establish the communication. The police sought leave to appeal on the basis the judge erred in his decision by: (1) applying language other than the statutory language in relation to serious emotional distress; and (2) concluding the evidence could not establish that distress.

Decision of the court

The court found that the prosecution had not established a prima facie case that the complainant in fact suffered harm as defined in section 4 of the HDCA 2015. The court held that the claimant was said to be 'frustrated, angry, anxious and very upset', and 'very depressed'; the claimant did not elaborate what she meant by 'depressed'. While the evidence clearly pointed to some degree of emotional distress, it was not sufficient to satisfy the court that it had reached the threshold of serious emotional distress. Furthermore, J's observation was not determinative of distress and therefore may have manifested itself later. The court emphasised that the claimant could have provided more detailed and specific evidence about her feelings or provided expert evidence from a psychologist or counsellor. On the second charge, the court disagreed with the lower court and argued that the judge had approached the issue of emotional distress by isolating the various descriptions of how the complainant felt, rather than – as defined by the statute – assessing the

evidence in its totality. The appeal was allowed and the lower court's decision to discharge the defendant was quashed.

Title: *Watchorn v R* [2014] NZCA 493

Weblink: Judgment

Issue: Accessing a computer system dishonestly.

Legislation

- Section 249(1) Crimes Act 1961

Facts

The defendant had been convicted on three charges under section 249(1) Crimes Act 1961 for allegedly accessing his employer's computer system dishonestly. He was an employee of an oil and gas company (TAG), which was engaged in oil and gas exploration. He downloaded extensive and sensitive geoscience data from the company's computer onto a portable hard drive. The information was of a high value and had it been disclosed to a competitor (NZEC), it would have been beneficial. On the day after the download, he and his family left to travel to Canada to visit his mother for four weeks. While in Canada, he met with representatives from NZEC – a competitor of his employer. Following this meeting, he was offered a job with NZEC.

The defendant later returned to work and downloaded more sensitive data onto a USB stick. He gave notice of his intention to resign and join the competitor. The claimant company was concerned about this, and its solicitors asked him to return the missing hard drive, reminding him of his obligations of confidentiality. The defendant responded stating that he only had technical data and work from his previous employment on his personal hard drive.

The police conducted search warrants on the premises of his former employer and interviewed the defendant, eventually arresting him. After interviewing the defendant, they found no evidence to suggest that he had disclosed the information downloaded to NZEC while he was in Canada. In the previous Court of Appeal decision of *Dixon v R* (2014) NZCA 329, the court held that digital CCTV footage was not 'property', as defined in section 249(1)(a) of the Crimes Act 1961. However, in this case, the issue was whether the court would follow the Dixon approach and include an alternative charge of obtaining a benefit.

Decision of the court

First, the court held that the defendant had accessed TAG's computer system and dishonestly or by deception and/or without claim of right, obtained a benefit per section 217 of the Crimes Act 1961 – given that he did not have TAG's authorisation to download the data onto his hard drive. The defendant's claim that he thought that he was authorised to download the files and take them to Canada was contrary to his version of events when interviewed by the police. Second, the court dismissed the defendant's defence that he had a claim of right to the data because he believed there was an industry-wide practice of downloading and transferring data relevant to the employee's work before leaving employment of the owner of the data. The court held that the defendant did not have a claim of right to the data, given that there was no evidence that implied entitlement did exist and no evidence that he believed that he did.

PAPUA NEW GUINEA

Title: *Mark v Neneo* [2019] PGNC 340; N8115 (22 November 2019)

Issue: The main issues for the court were: Has the plaintiff proved that the defendant breached her human rights? What orders should the court make?

Legislation:

- Cybercrime Code Act 2016
- Sections 37, 41 and 59 of the Constitution

Facts

The claimant, Dorothy Mark, was a journalist working at *The National* newspaper. She filed a complaint to the police that a member of the National Parliament of Papua New Guinea was guilty of offences under the Cybercrime Code Act 2016. This arose from the alleged publication of defamatory material about her on social media. The provincial police commander, the defendant, directed the claimant's complaint to the police force and advised her to consider pursuing her grievance through civil proceedings. Due to the inaction of the police force and the attitude and actions of the defendant, the claimant commenced proceedings against the defendant, claiming that they had stopped the police from investigating her complaint and had therefore breached her human rights under sections 37, 41 and 59 of the Constitution.

She sought declarations and an order that the provincial police commander would act on her complaint by bringing the Member of Parliament in for questioning for the alleged defamatory material, and an order that the defendant provide reasons for not acting on her complaint.

Decision of the court

The court argued that following Papua New Guinea (PNG) case law, members of the police force were under no general enforceable obligation to investigate a complaint of criminal conduct or to give reasons for their failure to investigate. As such, they had a wide discretion in deciding whether to investigate a complaint. The claimant's complaint was not an exceptionally serious one, sufficiently supported by evidence, and therefore did not give rise to an enforceable obligation on the part of the police to investigate. There was no breach of her human rights under sections 37, 41 and 59 of the Constitution. With the establishment that the claimant's rights had not been breached or would imminently be infringed, nor was there a reasonable probability of infringement, the proceedings were dismissed and no orders were made.

Title: *Kayapo v Hula* [2021] PGDC 235; DC7096 (22 December 2021)

Weblink: Judgment

Issue: The court needed to ascertain whether the evidence was satisfactory to charge the defendant for his alleged defamatory publication about the claimant.

Legislation:

- Section 21(2) of the Cyber Crime Code Act 2016
- Criminal Code Act 1974, Chapter 262
- Criminal Code (Amendment) Act 2016
- District Court Act 1963, Chapter 40

Facts

The defendant posted several comments on Facebook against the claimant, a member of the Lands and Physical Planning Ministry, alleging fraud on his part in acquiring the property title that had been previously occupied by the defendant and his family since 1989. The defendant was subsequently arrested and charged with the offence of defamatory publication using an electronic system or device, under section 21(1) and (2) of the Cyber Crime Code Act 2016, with the intention of injuring the reputation or profession/trade or ridicule of that person. The defendant argued that his actions of posting such comments against the claimant were protected and reasonable in law. He also relied on the defences contained in sections 21(5) and (6) of the Cyber Crime Code Act 2016, that the publication made was proper and was for the advantage of the public at large, made in good faith and a question of fact.

Decision of the court

Dismissing the case, the court ruled the defendant had sufficient evidence under section 21(6) to legitimately justify his defence under section 21(5)(vi) that his alleged defamatory publication under sections 21(1) and (2)(vii) was excused by law. There was documentation from an authorised authority to confirm that the defendant's publication was true.

Title: *State v Kakas [2021] PGNC 451; N9211 (14 October 2021)*

Weblink: Judgment

Issue: Cyber harassment.

Legislation

- Section 21(1)(a)(c)(i) of the Cybercrime Code Act 2016

Facts

The defendant, the former wife of the Secretary for the Department of Agriculture and Livestock, posted on Facebook details of how she was arrested by her ex when she went to serve him a family court summons. The claimant admitted that he had arrested his estranged wife due to some defamatory statement she had made about him on social media, which had defamed him and caused emotional distress. The state charged the defendant for cyber harassment, pursuant to section 23(1)(a)(c)(i) of the Cybercrime Code Act 2016, as she had used an electronic device with the intent to initiate and participate in communication and online discussions directly for the purpose of causing the defendant emotional distress. However, it was later found that the post the claimant was referring to was a different post on social media, where he was called a womaniser and drunkard. She appealed to the National Court, arguing that the evidence was lacking, tainted or discredited and that the indictment was bad for duplicity.

Decision of the court

Upholding the application, the court found that the evidence presented by the state was lacking, given that the cross examination revealed the claimant's complaint was about a different post. In terms of criminality, it followed that the post was not intended to cause emotional distress and not unlawful. Finally, the court held that the charge under section 21(1)(a)(c)(i) of the Cybercrime Code Act 2016 was bad for duplicity because it charged the claimant with initiating and participating in the offence. The application to stop the case was upheld and the claimant was acquitted and discharged of the indictment.

SAMOA

Title: *Police v Zhong* [2017] WSDC 7 (District Court)

Weblink Judgment

Issue: Money laundering.

Legislation

- Crimes Act 2013 s33, 161 and 165(b), 207, 213(a) of the Crimes Act 2013

Facts

Police conducted a search of a building following a complaint by a bank about suspicious activity involving its ATM machines. During the search, the police seized over 100 ATM cards, electronic tools and 3 electronic devices, including a skimming device used to copy, store and retrieve customer data. The police were looking for three Chinese national suspects. The search led to the arrest of two suspects. They faced several charges under the Crimes Act 2013. These consisted of 14 charges of theft, intentionally accessing an ATM machine without authority, accessing an ATM machine dishonestly and thereby obtaining $18,000.00 from the bank, and intentionally and without authorisation, possessing a card-skimming device designed for the purpose of committing an offence. Both defendants pleaded guilty to four charges at the commencement of trial. Two theft charges were withdrawn and dismissed on application by the prosecution, leaving them accused of a total of ten charges.

Decision of the court

The court found the two defendants guilty of eight theft charges amounting to $47,450. The court also found the two defendants guilty of dishonestly accessing an electronic system and thereby obtaining a benefit (section 207) and one charge of intentionally possessing a card-skimming device designed for the purpose of committing an offence. Both were sentenced to five years in jail.

TONGA

Title: *Rex v Hulita Potemani CR 166 of 2014*

Weblink: Judgment

Issue: Fraud.

Legislation

- Section 148(1) and (5) Criminal Offences Act
- Section 17(1)(a) and (b)(i) Money Laundering and Proceeds of Crime Act

Facts

The defendant, Mrs Potemani, accepted a friend request from one Mr Ikeatu on Facebook. She communicated with him on Facebook, text and telephone. He claimed that he lived in South Africa and to find common ground with her, claimed that he was of Tongan ethnicity and a Christian. The chats became intimate, and he said that he would travel to Tonga. He then asked the defendant if she could open a bank account for him so that he could advertise a product in Tonga and receive payments from clients. The defendant allowed him to use an existing account of hers and provided him with the bank account details. Funds were paid into her account, and she was then instructed by him to collect these funds and, through Western Union, send the money to him. Mr Ikeatu, or someone associated with him, had through computer hacking obtained the bank account details of the owners of a resort business in Tonga. They had successfully requested electronic transfers of 21,000 and 4,000 Tongan dollars (T$) from a couple's account (Mr and Mrs Holt) and paid the money into the defendant's account. The defendant tried to send the funds but was unable to as the bank became suspicious of her. Mr Ikeatu then instructed her to buy a laptop and other electronic goods to send to him. The bank then filed a suspicious transaction report under the Money Laundering and Proceeds of Crime Act 2000 and the defendant was charged. She voluntarily made statements to the police and assisted them with their investigation. The defendant faced one count of receiving, contrary to section 148(1) and (5) of the Criminal Offences

Act, and two counts of Money Laundering, contrary to section 17(a) and (b)(i) of the Money Laundering and Proceeds of Crime Act 2000.

Decision of the court

The court held that the defendant, beyond a reasonable doubt, had an actual belief that the money that she withdrew from the bank was stolen or obtained under circumstances which amounted to a criminal offence. There were several circumstances that should have put her on notice that the person from Facebook may have been involved in criminal activity – such as when he asked her to open a bank account for him after three days of speaking. If he was selling legitimate goods, the court stated that it would be expected for him to have a bank account. Furthermore, the defendant had lied to Western Union as to the reasons the money was being sent overseas, which indicated that she was aware of some criminal activity. She had also admitted to police that she thought the money was for marijuana. She was found guilty of the offence of receiving under section 148(1) and (5) Criminal Offences Act. On count two (money laundering), the court held that the charge was not proven because the Crown failed to prove that the money the defendant used to buy goods was derived directly or indirectly from criminal activities which amounts to a serious offence.

VANUATU

Title: *Public Prosecutor v Garae [2018]* VUSC 180; Criminal Case 1408 of 2018 (31 August 2018)

Weblink: Judgment

Issue: Extortion.

Legislation

- Section 138(f) of the Penal Code

Facts

During the time of their relationship, the defendant had requested that his girlfriend at the time take pictures of her genitalia and nude pictures and send them to him. This request was based on the understanding that the pictures would only be for his personal use and enjoyment. Soon after he received the pictures, he demanded the claimant buy credit for his mobile phone and then demanded cash transfers through Western Union. He threatened that if she did not comply, he would publish the nude pictures on Facebook. A total sum of 23,000 vatu (Vt) was extorted from the claimant. She reported the matter to the police after the defendant demanded a sum of Vt50,000. He was then arrested and under caution signed a voluntary statement in which he admitted the crimes.

The defendant was prosecuted on amended information that charged him with six (6) counts of extortion, contrary to section 138(f) of the Penal Code.

Decision of the court

The court found the defendant guilty of extortion, contrary to section 138(f) of the Penal Code, given that he made a threat to publish the claimant's compromising photographs on social media and demanded cash payments through threatening text messages. There was also a serious abuse of a trusting relationship in obtaining a sum of Vt23,000 from the vulnerable victim. The court described the offences as cruel, cowardly and mean-spirited. The defendant was sentenced to 13 months' imprisonment, ordered not to own, use or access a mobile phone that has an internet connection or capability, and ordered to pay compensation to the parents of the claimant.

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19104