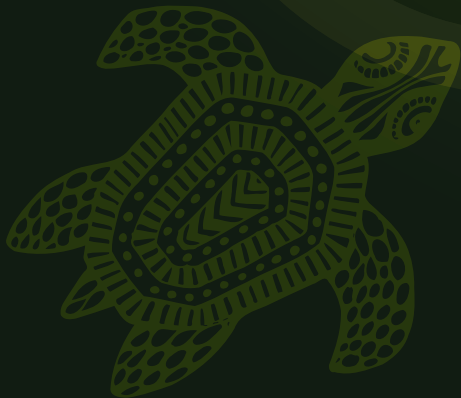


FOURTH ANNUAL PILON CYBERCRIME WORKSHOP, NADI, FIJI | 29 November to 2 December 2022

Combatting Cybercrime: Trends and Tools in a Changing World





FOURTH ANNUAL PILON CYBERCRIME WORKSHOP, [NADI, FIJI](#) | 29 November to 2 December 2022

CONTENTS

FOREWORD	2
INTRODUCTION	3
DAY 1 Stocktake of global trends in cybercrime	
Opening Ceremony, Prayer and Official Welcome	4
Session 1: Opening Remarks and Keynote Addresses	6
Session 2: Recent Trends in Cybercrime and Cyber-Enabled Crime in the Pacific	10
Session 3: Cybersecurity & Cyber Expertise - Countering New Threats	12
Day 1 End	15
DAY 2 Gendered aspects of cybercrime	
Session 1: Talanoa - Gendered Impacts of Social Media	18
Session 2: Pacific Perspectives on Law Reform	21
Session 3: Strategies for Supporting Victims of Cybercrime	22
Facts for Case Study 1 (Maria)	23
DAY 3 Operational tools	
Session 1: The Changing Digital Landscape: Safeguarding Pacific Communities in the Evolving Online World	28
Session 2: Digital Evidence and Mobile Phones	30
Session 3: Working Effectively with Expert Witnesses	34
Session 4: Focus on Financial Crimes: Key Issues with Electronic Evidence in the Pacific	32
Day 3 End	34
DAY 4 Bringing it All Together	
Background to the Zyber courses	37
Session 1: Zyber Panel Discussion on Case Study Outcomes	40
Session 2: Effective Legislation: Focus on Digital Evidence	41
Facts for Case Study 2 (Ngato)	42
Session 3: Case Study in Ransomware	49
Session 4: Pacific Cyber Stories: Legislation, Electronic Evidence and Prosecutions	50
Final Reflections and Closing Remarks	51
AGENDA	56
IN-PERSON PARTICIPANTS	58
EXTRA PHOTOS	60



FOREWORD

Mālō 'etau lava

It is my pleasure to introduce this booklet to you. Within its pages you will find an overview of the presentations and discussions we had across four days, as well as extracts from the case studies we explored.

My hope is that you will appreciate the central role which the PILON Cybercrime Workshop has played in enhancing linkages between Pacific law and justice agencies and providing a forum for attendees to expand their knowledge and skills and networks to more effectively combat cybercrime in our region.

Because this is the fourth and final Workshop under the grant provided by the Australian government, there are long-standing contributors I wish to acknowledge. Firstly, the governments of the respective host countries, Fiji, Vanuatu and our own Tonga. Secondly, the necessary funding provided by Australia through the Cyber and Critical Technology Cooperation Program. And finally, the Council of Europe who have always provided additional financial and technical support.

Our goal across every workshop has been to support our Pacific colleagues so that they might better cooperate to strengthen their legal frameworks and take steps to more effectively investigate and prosecute cybercrime.

As you review this booklet, I think you will agree we have achieved this goal.

Mrs. Linda Simiki Folaumoetu'i
Attorney General,
Kingdom of Tonga
Chair of the
PILON Cybercrime Working Group



INTRODUCTION

From 29 November to 2 December 2022, the Cybercrime Working Group of the **Pacific Islands Law Officers' Network (PILON)** held the fourth and final Annual PILON Cybercrime Workshop in Nadi, Fiji, together with the Office of the Attorney General (Republic of Fiji), the Australian Government's Cyber and Critical Technology Cooperation Program and the Council of Europe.

The annual PILON Cybercrime Workshop provides a valuable platform to gain insights into cybercrime challenges and opportunities for more effective collaboration across the entire justice system.

PILON provides a regional forum to discuss and progress law and justice issues common to countries within the Pacific. Combatting cybercrime is a key strategic priority, recognising that the borderless nature of cybercrime requires common legislative frameworks and international cooperation for effective prevention and prosecution. Bringing key stakeholders and experts together also responds to the call in the Boe Declaration for greater regional cooperation on cybersecurity.

This year's workshop explored the theme "Combatting Cybercrime: Trends and Tools in a Changing World". Attended in-person by over 60 police, prosecutors and cybercrime experts from 12 PILON member countries, we also had our colleagues join us online for the first time. Additionally, 26 prosecutors and police were also supported to undertake an online digital forensics training course delivered by Zyber/Insig2, with the certificate ceremony held during the Workshop on 2 December 2022.

The workshop emphasised the importance of identifying new and emerging trends since COVID 19, the gendered impacts of cybercrime, operational tools and legal policy responses to these trends. Participants were provided with a highly practically-focussed and collaborative agenda, offering insight into other countries' experiences of handling cases involving cyber and electronic evidence. Expert speakers came from Australian and Fiji online safety regulators, Australia's Commonwealth Director of Public Prosecutions, the Council of Europe, FBI, INTERPOL, PTCCC, Tonga Police, the Reserve Bank of Fiji and many others, each offered useful tips and resources on a variety of issues concerning the effective investigation and prosecution of cybercrime.

This booklet provides a visual snapshot and short text summary of these presentations and discussions.

We note this is the fourth and final in a series of flagship workshops funded by the Australian Cyber and Critical Technology Cooperation Program, with support from the Council of Europe. Looking ahead, PILON will continue planning new regional events to further explore issues important to PILON member countries.

If you would like further information or assistance, please contact coordinator@pilonsec.org or pilon@pilonsec.org.

OPENING CEREMONY

DAY 1



OPENING CEREMONY

1



Chief guests included (left to right): **Hon Ricky Muiakituki Makani** (Minister for Natural Resources, Niue), **Mrs Linda Folaumoetu'i**, (Attorney General, Kingdom of Tonga), **Ms Tupou'tuah Baravilala** (Acting Permanent Secretary of Communications, Republic of Fiji), **Mr Tobias Feakin** (Ambassador for Cyber Affairs and Critical Technology, Australia) and **Ms Su'a Hellene-Wallwork** (Attorney General, Independent State of Samoa)



DAY 1

Ms Tupou'tuah Baravilala**Acting Permanent Secretary of Communications, Fiji**<https://www.fiji.gov.fj/Media-Centre/Speeches/English/ADRESS-BY-THE-ACTING-PS-FOR-COMMUNICATIONS-TUPOU'T>

“ As the Ministry of Communications, I believe we have a bird’s eye view of how the whole cyber ecosystem comes together – from guaranteeing an enabling environment to ubiquitous access to connectivity, to digital transformation shifts, while at the same time ensuring cybersecurity safeguards are in place and measures to combat cybercrime. ”

“ The shift to online spaces has presented a challenge – the attack surface area has increased. Digital technologies continue to accelerate, and with it, cybersecurity risks continue to become more evident. We have seen emerging and evolving threats which are transboundary in nature and which have an impact on international peace and security and thereby, placing cybersecurity as a priority. ”

“ At a national level, we are in the process of reviewing our National Cybersecurity Strategy, establishing our national Computer Emergency Response Team and to formalise the current capabilities that exist. ”

“ The Fijian Parliament enacted the Cybercrime Act which is aligned to the Budapest Convention on Cybercrime. The Budapest Convention is the gold standard and is the only international instrument that deals with cybercrime and electronic evidence. ”



SESSION ONE - KEYNOTE PRESENTATION



THE VALUE OF
BRINGING PEOPLE
TOGETHER



PRACTICAL
OUTCOMES



WE HAVE ACHIEVED
SO MUCH ACROSS
the REGION in TERMS
of STANDARDS,
LEGISLATION &
EDUCATION



CYBERCRIME
CONTINUES to
INCREASE ...

and AFFECTS not ONLY the
VICTIM, but OUR INFRASTRUCTURE...
and HAS a RIPPLE EFFECT in TERMS
of ERRODING TRUST.



SHARING STORIES
& CASE STUDIES



TECH TRAINING,

POLICY ADVICE,



STANDARDS



WE NEED to WORK
TOGETHER for the
SAFETY & SECURITY
of OUR PEOPLE,
& VIABILITY of
OUR ECONOMY

Dr Tobias Feakin

Australian Ambassador for Cyber Affairs and Critical Technology

“ Prosecuting cybercrime continues to be a challenge in our region, and across the globe – and the urgency of this task is only increasing as our communities become more connected. ”

“ Cybercrime is often talked about as a fundamentally different challenge to anything law enforcement agencies have faced before, requiring innovation to respond to the rapid pace of technological change. ”

“ But we must not discount the importance of robust fundamentals, including law enforcement cooperation, information sharing, and stronger partnerships across the justice system. ”

“ The PILON Cybercrime Working Group is integral to driving this work forward in the Pacific. ”

“ I want to thank you again for joining us here in Fiji and online for the PILON Cybercrime Workshop. I am very much looking forward to the discussion today, and to our continued cooperation to build a vibrant region in cyberspace. ”





SESSION ONE - KEYNOTE PRESENTATION



WE NEED TO WORK TOGETHER... and WE CAN RISE TO THE CHALLENGE



WE HAVE MORE CONNECTED DEVICES than EVER. 95% in FIJI



IT IS KEY THAT WE CONTINUE TO COLLABORATE REGIONALLY & GLOBALLY, TO LEVERAGE EXISTING WORK & SHARE STORIES



WE ANTICIPATE 145M NEW DIGITAL JOBS by 2025



REQUIRES a PIPELINE OF SKILLS



AND OF SECURITY & LEGISLATION

THIS IS HOW WE COMBAT CYBERCRIME

DAY 1

This section of the booklet covers Day 1 Presentations ("Stocktake of Global Trends in Cybercrime") which included

- **Session 2:** Recent Trends in Cybercrime and Cyber-Enabled Crime in the Pacific
- **Session 2 (cont.):** International Cooperation on Emerging Threats - Child Exploitation Developments During the Pandemic
- **Session 3:** Cybersecurity & Cyber Expertise - Countering New Threats



CYBER THREAT LANDSCAPE WEI XIAN TEE



PHISHING

- AS-a-SERVICE
 - MORE TIME WPH = MORE ATTACKS
- CAPITALISE ON COVID
- from \$20USD!



E-COMMERCE DATA INTERCEPTIONS

SHIFT from ATMs / POS

CARDING MARKET GREW by 116%.



CRIMEWARE as a SERVICE

↓ BARRIER to ENTRY for LESS TECH-SAVVY CRIM'S.



BEC BUSINESS EMAIL COMPROMISE

- 1 HACKING
- 2 SOCIAL ENGINEERING FRAUD
- 3 MONEY LAUNDERING

TARGETS

→ INFO STEALERS

→ RATS



INDIVIDUAL COMPANY

1.49m GLOBAL DETECTION



RANSOMWARE

BANKING, HEALTHCARE, TELCO'S

* >3.7m DETECTIONS

CRYPTO SCAMS & CRYPTO JACKING

STEAL INFO

MINE CURRENCY

RANSOMWARE has EVOLVED...

1989 → Today



RECENT TRENDS in CYBERCRIME in the PACIFIC

MICHAEL CROWE

OUR LEADERS AGREE CYBER SECURITY REQUIRES URGENT ATTENTION

IT is a KEY FOCUS AREA, & PROPOSED ACTIONS to be REVIEWED SHORTLY.

COLLABORATION is KEY! DEVELOP RELATIONSHIPS with MINISTRIES to CONTINUE the NETWORK GROWTH

IT is PART of OUR 2050 VISION

PEACE and SECURITY

TECH and CONNECTIVITY



WE NEED WHOLE of GOV'T & WHOLE of REGION COLLABORATION

OUR PROPOSED ACTIONS...

WE NEED YOUR HELP!

BUDAPEST CONVENTION

SHARING INFORMATION

NATIONAL CYBER POLICIES/STRATEGIES / LEGISLATION

AWARENESS & EDUCATION

CERT CAPACITIES



This session provided a high-level overview of global trends and how these are flowing through to the Pacific, helping attendees understand what the emerging threats are which may require a regulatory response. Mr Wei Xian Tee (Cybercrime Specialist, Digital Investigation Support, Cybercrime Directorate, Interpol) from Interpol's Singapore bureau highlighted some recent notable trends in cybercrime for participants, including topics such as ransomware and business email compromise that were considered in greater depth later in the Workshop.

Mr Michael Crowe (Regional Security Advisor, Pacific Islands Forum Secretariat, above) and Sergeant Titimaea Nemaia (Member, Pacific Transnational Crime Coordination Centre) then explained some of the strategic and operational collaboration taking place in the Pacific to respond to these ever-evolving threats, including under the Boe Declaration Action Plan and the 2050 Strategy. No one can do it alone and collaboration is key!



PACIFIC TRANSNATIONAL CRIME COORDINATION CENTRE

TITIMAEA NEMAIA



est. 2002

A MULTI-AGENCY APPROACH to TARGET TRANSNATIONAL CRIME

NO ONE CAN DO IT ALONE!

KEY FUNCTIONS of PTCCC

INFO COORDINATION

INTELLIGENCE PRODUCTS

COLLABORATION & PARTNERSHIPS

CAPABILITY DEVELOPMENT

CHALLENGES

ACCESS to DEVICES & CONNECTION...

but LACK of AWARENESS & EDUCATION

LACK of RELEVANT LEGISLATION

CYBERCRIME AFFECTS everyone...

3rd MOST REPORTED TRANS-NAT. CRIME!

AND the THREAT CONTINUES to GROW IN NUMBERS & VARIATION



IDENTIFIED ACTIONS

- PUBLIC EDUCATION
- LAW ENF'T EDUCATION
- INFO SHARING
- COLLABORATION
- LEGISLATION



INTERNATIONAL COOPERATION: CHILD EXPLOITATION

INTERPOL



195 MEMBER COUNTRIES CONNECTED



- SECURE COMMS
- COMMON GOALS
- LOCAL ACTION
- TRAINING/CAPACITY BUILDING
- ACCESS to DATABASES

inc. CHILD EXPLOITATION DATABASE



"ICSE"

ALLOWS COUNTRIES TO UPLOAD and ANALYSE DATA



11010101
10101101
101101

INTERPOL NOTICES

- WANTED PERSONS
- INTELLIGENCE
- WARNING OF KNOWN CRIMINALS
- MISSING PERSONS
- UNIDENTIFIED BODIES
- THREATS
- MODUS-OPERANDI
- SPECIAL INTERPOL-UN SECURITY COUNCIL

PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

JESSAMY GEE '22

After hearing about global trends in cybercrime, attendees then considered how international cooperation between law and justice agencies under relevant regional and international frameworks facilitates responses to one of the most serious cybercrime threats: child exploitation.

In this session, In this session, the Australian Federal Police National Central Bureau and **Mr Dean Chappell** (Assistant Legal Attache,

Federal Bureau of Investigation) spoke about how police-to-police and mutual assistance requests can be used to counter child exploitation.

Mr Damian Rapira-Davies (Lead Operational Advisor, Digital Safety, Regulatory Services, Te Tari Taiwhenua Department of Internal Affairs) also highlighted how New Zealand is working with Pacific regional partners to implement a technical solution in their jurisdictions.

INTERNATIONAL COOPERATION: CHILD EXPLOITATION

DEAN CHAPPELL

VCAC INTERNATIONAL TASK FORCE

- SHARING INFO & INTELLIGENCE
- LEVERAGING NETWORKS
- SHARE BEST PRACTICE
- TRAINING
- ACCESS TO EXPERTS



WE CAN ONLY SUCCEED BY WORKING TOGETHER

BUILDING RELATIONSHIPS & UNDERSTANDING

NCMEC

- DATABASE that's CONSTANTLY UPDATED
- ONLINE RESOURCES and TRAINING
- YOU CAN LEVERAGE THIS TOO!

TRENDS

- ENCRYPTION**
DON'T GIVE UP! ALWAYS ASK!
- CHILD-LIKE SEX DOLLS**
OFTEN LEADS TO CSAM
- LOCATION SERVICES**
- CRYPTOCURRENCY**
THE NUANCES MATTER for IDENTIFICATION
- NEW COMPANIES**
TIME to EDUCATE on SAFETY
- PREFERENCE for VIDEO**
- OFFENDER is USUALLY KNOWN** to the VICTIM

SUPPORTING C.E. INVESTIGATIONS] FIND LINKAGES, EVIDENCE, POLICE-to-POLICE, then MLAT
ALL YOU HAVE TO DO IS ASK!



INTERNATIONAL COOPERATION: CHILD EXPLOITATION

DAMIAN RAPIRA-DAVIES



THE DIGITAL SAFETY GROUP

ANALYSTS, ADVISORS, INVESTIGATORS & SMES SURROUNDED BY GLOBAL NETWORK



LEVERAGE & SHARE TECH & DATA SETS



WE CANNOT DO IT ALONE!

FUNCTIONS: ENFORCE the FILM, VIDEOS & PUBLICATIONS CLASSIFICATION ACT 1995

INVESTIGATE OFFENSES

SUPPORT the 11 VOLUNTARY PRINCIPLES to COMBAT CSE

RELATIONSHIPS with SERVICE PROVIDERS

HOW COULD YOU LEGISLATE COOPERATION in YOUR COUNTRY?



DIGITAL FILTERING SYSTEM: REGULARLY REVIEWED BLOCK LIST that PREVENTS ACCESS to OBJECTIONABLE SITES

TRIAGING REFERRALS

STARTS with AUTOMATION, then CONSIDERS...

- CRIMINAL HISTORY
- ACCESS to CHILDREN
- IDENTIFICATION
- KNOWLEDGE

REPORTS VIA

- NCMEC
- NETSAFE
- OCET MAILBOX
- ONLINE COMPLAINTS SYSTEM



SIGNIFICANT INCREASE in REFERRALS DURING COVID

The final session of the day provided an overview of how cybercriminals are currently targeting Pacific organisations and the key cybersecurity trends that law and justice agencies need to be aware of.

Dr Jeffrey Garae (Director, CERT VU and Chair, Pacific Cybersecurity Operational Network) outlined effective regional collaboration approaches and successful country-level responses to new or recent cyber threats.

We then asked "How can CERTs and information sharing assist police (and prosecutors) in their roles?"

An ongoing question was how legal and police professionals could work effectively with cybersecurity experts to investigate and prosecute cybercrime offences. To answer this, our speakers **Mr Enoka Feterika** (Cybersecurity Advisor, Pacific Island Chiefs of Police/Cyber Safety Pasifika representative) and **Chief Superintendent Kalisi Tohifolau** (Tonga Police) explored the best strategies for recognising the point where this expertise adds value, and directed attendees toward key resources.



CYBER SECURITY & EXPERTISE COUNTERING NEW THREATS

DR. JEFFERY GARAE, CHIEF SUPERINTENDENT KALISI TOHIFOLAU & ENOKA FETERIKA

CYBERCRIME OVERVIEW

- 3 NEW PIECES OF MALWARE EVERY SECOND
- RANSOMWARE GREW BY 150% IN 2020
- THE NUMBER & SOPHISTICATION OF ATTACKS CONTINUES TO INCREASE

THREAT LANDSCAPE

EMOTET & BEC, MALWARE, SEXTORTION, PHISHING, DIS/MISINFORMATION, INSIDER THREAT, DATA BREACH, RANSOMWARE, DATING SCAMS



REGIONAL RESPONSE

COLLABORATION, PARTNERSHIPS, TREATIES & AGREEMENTS

COUNTRY-LEVEL RESPONSE

NATIONAL POLICIES, STRATEGIES, LEGISLATION & FRAMEWORKS

BEST PRACTICE

- INVESTIGATION & DIGITAL FORENSICS SOPs
- PROMOTE AWARENESS
- INFO SHARING & CAPACITY BUILDING



CERTs, AGO, INT. AFFAIRS, ISPs, FINANCIAL INTEL., NGOs (COUNSELLING), WORKING GROUPS, INTER-AGENCY COOPERATION

INTERNATIONAL COOPERATION

INFORMAL FORMAL
START HERE!



COOPERATION & COLLABORATION...
THE ONLY WAY FORWARD!

CYBER SAFETY PASIFIKA (CSP)

- AWARENESS & EDUCATION
- UPSILLING POLICE
- LEGISLATION & POLICY

IN COLLABORATION w- GOV'T, POLICE, FBI

- ONLINE TRAINING - REAL LIFE, CONTEXTUAL EXAMPLES
- THE BASICS

OUR SAFETY IS EVERYONE'S RESPONSIBILITY - INCLUDE ISPs IN TRAINING & LEGISLATION?

PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

JESSAMY GEE '22



DAY 1 END





Day 1 was concluded with remarks from (anticlockwise from top right): **Glenys Andrews** (Office of the Attorney General, Republic of Fiji), **Mrs Linda Folaumoetu'i**, (Attorney General, Kingdom of Tonga), **Ms Ana Elefterescu** (Council of Europe) and **Ms Pirjo-Liisa Heikkila** (Delegation of the European Union for the Pacific) before the meal was opened by **Alan Rua** (Cook Islands Police).

Participants enjoyed a traditional Fijian meke, involving dancers, singers and percussionists.

DAY 1 END



DAY 2

GENDERED ASPECTS OF CYBERCRIME

This section of the booklet covers Day 2 Presentations ("Gendered Aspects of Cybercrime") which included

- **Session 1:** Talanoa - Gendered Impacts of Social Media
- **Session 2:** Pacific Perspectives on Law Reform
- **Session 3:** Strategies for Supporting Victims of Cybercrime



TALANOA - GENDERED IMPACTS OF SOCIAL MEDIA

E-SAFETY COMMISSIONER AUSTRALIA

KIRA OSBORNE



ONLINE VIOLENCE AGAINST WOMEN is a GLOBAL CHALLENGE

85% OVERALL PREVALENCE

WOMEN are DISPROPORTIONALLY TARGETED

WE NEED a MULTISECTORAL RESPONSE & REGIONAL APPROACH

TECHNOLOGY FACILITATED ABUSE (TFA)



4 in 5 WOMEN



UNDER-REPORTED for MANY REASONS, inc. FEAR & SHAME

COMMUNICATION LOOP w- WOMEN to ↑ AWARENESS & RECEIVE INFO ON HOW THEY'RE EXPERIENCING TFA



ROBUST & UP-TO-DATE DATA. LISTEN to their STORIES!

PREVENTION



AWARENESS & EDUCATION

PROACTIVE and SYSTEMIC CHANGE



BASIC ONLINE SAFETY EXPECTATIONS and CODES



SAFETY by DESIGN

PROTECTION ONLINE SAFETY ACT COMPLIANCE & ENFORCEMENT ACTIONS





TALANOA - GENDERED IMPACTS of SOCIAL MEDIA

FIJI ONLINE SAFETY COMMISSION

TAJESHWARI DEVI

FACTORS to CONSIDER to ASSESS HARM

- EXTREMITY of LANGUAGE / IMAGES / VIDEOS
- AGE & CHARACTERISTICS
- ANONYMITY
- REPETITION
- TRUE / FALSE
- CONTEXT



STAKEHOLDER ENGAGEMENT & RELATIONSHIPS are everything

INVESTIGATIONS

- ✓ SEEK to RESOLVE
- SERVE a NOTICE
- ADVISE the PERSON MAKING the COMPLAINT

PARTNERS

- e SAFETY COMMISSIONER AUSTRALIA RESOURCES + NETWORKS
- FIJI POLICE FORCE INVESTIGATING, TRAINING and AWARENESS

REPORTS

- 60% FEMALE
- 36% FACEBOOK
- 6% TIK TOK
- GENDER-SPECIFIC HARASSMENT
- UNDER-REPORTING for MINORS as THEY REQUIRE an ADULT to REPORT

Day Two of the Workshop focused on the gendered aspects of cybercrime in the Pacific. The first session explored technology-facilitated abuse facilitated by social media, and the broader cultural and social considerations in a Pacific context.

Our first speaker **Ms Kira Osborne** (Pacific Lead, Australia's eSafety Commissioner) covered the post-pandemic outlook in the online safety space, explained the specific risks for women and girls and outlined Australia's regulatory framework concerning online safety in Australia.

Ms Tajeshwari Devi (Senior Executive, Fiji Online Safety Commission) and **Corporal Savenaca Siwatibau** (Digital Forensics / IT Investigation / Cybersecurity, Ministry of Defence, National Security and Policing) from Fiji Police then explained the key features of Fiji's regulatory model for online safety, including the significant education and awareness outreach conducted by their two agencies.



TALANOA - GENDERED IMPACTS of SOCIAL MEDIA

FIJI POLICE FORCE

CORPORAL SAVENACA SIWATIBAU

DIGITAL LITERACY & ONLINE SAFETY



MoUs with our PARTNERS to be CLEAR on ROLES

WE WORK TOGETHER as a FAMILY



collaborate WITH ISPs, MEDIA, PODCASTS, SCHOOLS

TAKE EVERY OPPORTUNITY! EMPOWER our COMMUNITIES!



FIJI is NOW 95% CONNECTED ... So WE HAVE a DUTY to KEEP PEOPLE SAFE.

RECOGNISE and MAXIMISE your STRENGTHS

- COMMUNITY ENGAGEMENT & AWARENESS
- POLICE TRAINING
- UPGRADE FORENSIC TECHNOLOGY
- CAPACITY BUILDING

VISIT THEM & GIVE them OWNERSHIP

DAY 2

The second session of **Day Two** then turned to recent legal developments or law and justice initiatives concerning cybercrime and its impact on women and girls. This session was focussed on hearing stories from Pacific jurisdictions on recent legal developments or law and justice initiatives concerning cybercrime and its impact on women and girls.



TALANOA - GENDERED IMPACTS of SOCIAL MEDIA

WOMEN & GIRLS FACE SPECIFIC THREATS ONLINE...



but THERE is a REDUCED NUMBER of REPORTS

- AWARENESS & EDUCATION
- CONSTANT EXPOSURE
- REPRESENTATION in CRIMINAL JUSTICE SYSTEM. = FEELING COMFORTABLE to REPORT.

RIGHTS
↑
SPECIAL TRAINING



A VICTIM-CENTRIC APPROACH



TALANOA - GENDERED IMPACTS of SOCIAL MEDIA



ONLINE SAFETY



CYBER SECURITY

→ FIRST LINE of DEFENCE for →

KNOWING WHAT to DO & HOW to ACT ONLINE, e.g.

- DIGITAL LITERACY
- PASSWORDS
- MENTALITY SHIFT (AWAY from "I DON'T CARE, IT DOESN'T AFFECT ME")



THE THRESHOLD / DEFINITIONS WILL be CONTEXTUAL
SEEK FEEDBACK from COMMUNITIES to ADDRESS THEIR ISSUES.

WE'RE THERE to SERVE THEM.

RELATIONSHIPS w- SOCIAL MEDIA
BE PERSISTENT. LEVERAGE YOUR PACIFIC HOSPITALITY... THE HUMAN FACTOR.
USE YOUR STRENGTHS.

THERE are MECHANISMS & PACIFIC TEAMS. APPROACH AS A REGION. LEVERAGE LEGISLATION to SET EXPECTATIONS.



EVIDENCE & RESEARCH

REGIONAL ORGS WILL NEED to TAKE THIS on in THE PACIFIC, so OUR RESOURCES & RESPONSE CAN BE FIT for PURPOSE



TRANSLATE RESOURCES to LOCAL LANGUAGES





PACIFIC PERSPECTIVES on LAW REFORM

JOSEPHINE ADVENT PITMUR (PNG)

IMAGE BASED ABUSE OF SORcery ACCUSATION RELATED VIOLENCE (SARV)

WHAT IS SORcery or WITCHCRAFT?

BELIEF & PRACTICES that ONE HUMAN CAN HARM ANOTHER by MAGICAL / SUPERNATURAL MEANS (OFTEN AROUND ILLNESS or DEATH)

IMPLICATIONS for HARM CAN be VERY SERIOUS, inc. TORTURE for CONFESSION

OUR MESSAGE - THE RULE OF LAW PREVAILS. YOU CAN HAVE your BELIEFS but NOT at the EXPENSE of a LIFE.

WHAT WILL STOP SARV?

- PREPAREDNESS OF INDIVIDUALS
- COOPERATION X-SOCIETY
- COMMUNITY LEADERSHIP
- COMPASSION



SARV IMPACTS EVERYONE ... but the KIND of VIOLENCE on MEN / WOMEN is DIFFERENT

IMPACT DIFFERS REGIONALLY



WOMEN are MORE LIKELY to FACE VIOLENCE or be DISPLACED

ACTION AREAS

- SERVICES
- ADVOCACY & COMM'S
- LEGAL + PROTECTION
- RESEARCH

*TARGETED TRAINING on STATEMENT WRITING



SHARING IMAGES without CONSENT on SOCIAL MEDIA or IN COMMUNITIES

SARV IMPACTS the WHOLE FAMILY

CHILDREN are MOST AFFECTED

IT ERODES TRUST.

SARV is COMPLEX

CULTURE + WORLDVIEW e.g. REVENGE CULTURE, POLYGAMY / JEALOUSY...

- LOCAL NARRATIVE
- RELIGION
- LOCAL CONTEXT
- RULE OF LAW



PACIFIC PERSPECTIVES on LAW REFORM

ANDREW KELESI (SOLOMON ISLANDS)

SOLOMON ISLANDS

OUR CURRENT POSITION

2 LEGISLATIONS that DEAL with DIGITAL EVIDENCE:

- EVIDENCE ACT 2009
- POLICE ACT 2013

- * SAFEGUARDS are INADEQUATE
- * LAW REVIEW is IMPERATIVE

WE are RUNNING BEHIND, but LOOK FORWARD to LEARNING from OTHERS

COMMON ISSUES

BULLYING & HARRASSMENT that CAN LEAD to HARM

SHARING POLITICAL / DISRESPECTFUL COMMENTARY

* CURRENT LAWS ONLY RELATE to IMAGES



COLLECTION & ADMISSION of ELECTRONIC EVIDENCE



NEEDS to be INCLUDED in LEGISLATION

Ms Josephine Pitmur (Deputy Secretary, PNG Department of Justice and Attorney General) presented on the role of social media in amplifying sorcery-related violence and related attacks on women and girls, and any legal or policy responses that PNG has developed (or is considering) to respond to these trends.

Mr Andrew Kelesi (Deputy Director of Public Prosecutions, Solomon Islands Office of the Director of Public Prosecutions) then presented on the Evidence Act 2009 (Solomon Islands) and challenges with electronic evidence in recent cases from the Solomon Islands, with particular focus on cases impacting women and girls. This presentation included thoughts on planned reforms and training, which drew thoughtful contributions from the audience.

DAY 2 – FIRST CASE STUDY SESSION

In our first case study session of the Workshop, participants navigated an interactive exercise focused on building a holistic understanding of victim pathways through the legal framework regulating cyberbullying and image-based abuse. The exercise was adapted from an earlier case study used in the Zyber 'Fundamentals of Digital Forensics' online training courses. During this adapted case study, the audience was invited to explore how a victim's experience can be framed or shaped by the support they access at various stages, and the role of prosecutors and police in assisting victims to navigate the process.

This session was facilitated by **Ms Stephanie Dunn** (Legal Officer, Fiji Women's Crisis Centre) and **Ms Lavonne Goundar** (Assistant Counsellor Supervisor, Fiji Women's Crisis Centre). **Chief Superintendent Kalisi Tohifolau** (Commander, National Crime and Investigations, Tonga Police) outlined recommendations for how police can handle complaints by victims of image-based abuse in a sensitive manner.

Ms Mercy Tamate (Prosecutor-in-Charge, Family and Sexual Violence Unit, PNG OPP) also shared recommendations for how prosecutors, police and witness support officers can work together to support vulnerable witnesses throughout the prosecution process, drawing upon her experience and the PILON SGBV Advisory Panel's work on the Regional Guidelines for Prosecutors and Witness Support Officers.



STRATEGIES for SUPPORTING VICTIMS of CYBERCRIME



MORAL SUPPORT
THROUGHOUT the
PROCESSES for a
SURVIVOR WITNESS
PREVENT RELIVING
T R A U M A

YOU ARE
PART of
the JUSTICE
SYSTEM

WITH THEM on the WHOLE
JOURNEY, through ALL
SERVICES & POST-PROSECUTION
IT IS A LONG PROCESS



NEVER FORGET the
HUMAN ASPECT

ENGAGE our
COMMUNITIES
to UNDERSTAND

MAKE the
NECESSARY
REFERRALS
WHEN you DON'T
HAVE the SKILLS



WE MUST BUILD CAPACITY the WHOLE WAY through: FROM FRONTLINE
to PROSECUTION

ALL STAKEHOLDERS MUST TREAT VULNERABLE
WITNESSES with EMPATHY, DIGNITY & RESPECT



PACIFIC ISLANDS LAW OFFICERS NETWORK – CYBERCRIME WORKSHOP 2022

JESSAM'S GE



CASE STUDIES



FACTS FOR CASE STUDY **ONE** (MARIA)

Maria (15) and Kai (17) live in Oceania and have been in a relationship for a few months. They met through Kai's friend Bob (18). One day when Bob was hanging out with Kai at his house, Bob downloaded and installed hacking software onto Kai's laptop to capture all of his social media passwords. This software was discreet, so Kai didn't notice anything.

A few days later, the hacking software sent all of Kai's passwords to Bob's phone, including his Facebook password. Bob's wife was down at home so he went to the library to use one of their computers. He logged onto Kai's Facebook and pretending to be him, messaged Maria asking for nude pictures. Maria and Kai had previously exchanged nude pictures of themselves online, so Maria took some photos on her phone and sent them to Kai on Facebook messenger.

Once Bob received the photos on Kai's account, he uploaded them to Explicit.com, a website which illegally holds explicit sexual pictures. Explicit.com paid Bob for providing the pictures. To ensure Kai didn't find out what happened, Bob deleted Kai's Facebook account, logged off the library computer and went home.

FACTS FOR CASE STUDY ONE (MARIA)

Maria found out that the pictures were circulating online from a mutual friend and broke up with Kai, who insisted that he didn't know anything about them and hadn't shared them any further. Kai tried to log into Facebook to find out what had happened, only to discover his account had been deleted.

Noticing that Maria was upset, her parents found out what happened and made a complaint to the police. At the station, while giving her statement, Maria's mother noticed that she looked very distressed and had difficulty in concentrating when she was being asked questions about the incident. The mother quietly signalled to the Police Officer for a break but the police officer informed her that she was only delaying the process of investigation and the arrest of the perpetrator.

The mother kept quiet after that and the police officer continued taking Maria's statement. Once the statement was done, Maria and her mother made their way out of the station. As they were leaving, they overheard the police officer telling the other officers that Maria had no values and that she was an embarrassment to their culture for sending nudes.

The police arrested Kai and brought him in for questioning. Further investigation following the interview with Kai uncovers the ISP address of the library computer which was used to upload the photos. Further enquiries at the library lead police to Bob. When he sees the police walk up to his house, Bob quickly deletes the passwords and the Explicit.com app from his phone, which he has used to view the pictures several times since he uploaded them.

The nudes have spread throughout the school and some of Maria's extended family and class mates have ridiculed her for it. The school administration has also put her on suspension because she had shared nude images which went against the school's values. Maria had become withdrawn and was self-harming. Her family feared that she was becoming suicidal. Maria and her parents have decided that they do not want to proceed with the complaint.

The police have proceeded to charge Bob with a number of offences but he is maintaining his innocence. The police is finding it difficult to get in contact with Maria and her family.

DAY 2



STRATEGIES for SUPPORTING VICTIMS of CYBERCRIME CASE STUDY



PROCEDURE IMPROVEMENTS

- ACKNOWLEDGE PSYCHOLOGICAL ASPECTS & WELLBEING OF SURVIVOR
- TRAUMA-INFORMED, SAFE SPACE. OFFER FEMALE OFFICER.
- ASK their PREFERENCE & ENSURE COMFORT
- EMPOWER SURVIVOR to TELL HER STORY.
- SURVIVOR SUPPORT ROLE (OUTSIDE OF FAMILY?)
- TALK to MUM SEPARATELY
- BUILD TRUST & RAPPORT
- DO NOT RUSH
- BALANCE with ENSURING RIGHT Q'S are ASKED & NO ASSUMPTIONS
- TAKE BREAKS as REQUIRED
- OUT of UNIFORM?
- PROVIDE ADVICE for NEXT STEPS and CHECK IN with VICTIM

IMPROVES QUALITY of the STATEMENT, WHICH AFFECTS PROSECUTION.

WE MUST RECOGNISE the CULTURAL & RELIGIOUS CONTEXT WE are in, and the GENDERED IMPLICATIONS

SAFETY of the SURVIVOR is PRIORITY → CONNECT to SERVICES

APPROACH from the HUMAN ASPECT



NOT TREATING the SURVIVOR RESPECTFULLY, LEADS them to FEEL... EMBARRASSED, HUMILIATED, ASHAMED, TRAUMATISED, VIOLATED, UNSUPPORTED ... WHICH DOESN'T LEAD to an OPEN & FRANK STATEMENT



STRATEGIES for SUPPORTING VICTIMS of CYBERCRIME CASE STUDY



THE FLOW-ON IMPACTS in HER SCHOOL and COMMUNITY are SEVERELY AFFECTING MARIA'S MENTAL HEALTH

MARIA & HER FAMILY DECIDE NOT to PROCEED.

THE POLICE HAVE CHARGED BOB & FINDING it HARD to CONTACT MARIA

DIGITAL EVIDENCE CONSIDERATIONS



IDENTIFY OFFENCES CONSIDERATIONS



The final component of this session featured an audience discussion to cover key takeaways from the exercise, including differences between jurisdictions and the balance between support structures and legal provisions. Audience members were asked:

- **How will** certain responses be perceived by the victim? Could this affect their willingness to continue with the complaint?
- **What is** the role of the police officer, support officer and prosecutor and what are the key points of communication to ensure the process works smoothly?
- **Where can** each process reinforce and support the central objective of moving toward a fair hearing for the complaint?
- **Would they** respond differently based on the victim's characteristics (e.g. if they were a child or elderly person)



STRATEGIES for SUPPORTING VICTIMS of CYBERCRIME CASE STUDY



PREPARING the SURVIVOR / VULNERABLE WITNESS for TESTIMONY is KEY → MAKE them COMFORTABLE → SAFE ENVIRONMENT → KEEP in CONTACT

SPECIAL MEASURES for TRIAL



DAY 3

THE CHANGING DIGITAL LANDSCAPE

This section of the booklet covers Day 3 Presentations ("Operational Tools") which included

- **Session 1:** The Changing Digital Landscape: Safeguarding Pacific Communities in the Evolving Online World
- **Session 2:** Digital Evidence and Mobile Phones
- **Session 3:** Working Effectively with Expert Witnesses
- **Session 4:** Focus on Financial Crimes: Key Issues with Electronic Evidence in the Pacific



THE CHANGING DIGITAL LANDSCAPE NICOLE MATEJIC



PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

JESSAMY GEE '22

Day Three opened with an examination of the changing digital landscape and the implications for cybercrime. **Nicole Matejic** (Principal Policy Advisor, New Zealand Department of Internal Affairs Te Tari Taiwhenua) explained ethical and regulatory issues created by the Metaverse and similar platforms.



Jope Tarai (Ph.D. Student, Department of Pacific Affairs, Australian National University) shared statistics underlining the shifting fault lines in the digital landscape. Reflecting the Pacific's "Youth Bulge", Jope observed that the 18 to 30-year-old age group in the Pacific constituted the majority of Facebook and Instagram users. Dovetailing with Day 2's consideration of the gendered aspects of cybercrime, Jope also identified that female identified users now account for the majority in at least 12 of the 18 countries reviewed.



THE CHANGING DIGITAL LANDSCAPE JOPE TARAI

INTERNET ACCESS in the PACIFIC is **GROWING**

AS is **MOBILE PENETRATION**

ENGAGEMENT w- **SOCIAL MEDIA**

THE DIVIDE is **SHRINKING**
* UNDERSEA CABLES * COVID IMPACT
BUT the LITERACY/SAFETY DIVIDE REQUIRES RESEARCH

ESTIMATED AUDIENCE 2.1-2.4m
MAINLY in **MAJOR CITIES**



TOP COUNTRIES
PNG, FIJI, NC, SAMOA



TOP PAGES
LOCAL NEWS, MEDIA & GOV'T

PACIFIC TRENDS
SLIGHTLY FEMALE DOMINATED
WHY? WHAT RISKS/CHALLENGES DOES IT BRING?

DIGITAL NATIVES 18-30 are the **MAJORITY**

WE NEED to ENGAGE these AUDIENCES



MORE SUPPORT FOR RESEARCH NEEDED

DAY 3

Siosaia Vaipuna (Director, Pacific GFCE (Global Forum on Cyber Expertise) Hub) then explained how the Global Forum on Cyber Expertise can assist PILON members to share, coordinate and strengthen resources when considering how to combat emerging threats.



Further sessions in Day 3 invited the audience to consider how we move from understanding the broader environment to considering how that translates into the Pacific's law and justice response. Session 2 discussed the challenges experienced by digital forensics examiners when extracting evidence from mobile phones. Using a practical exercise involving a case study, **Michael Callan** (Council of Europe, and Australian Fraud and Anti-Corruption Academy) explained how these challenges are addressed during the investigation, as well as the procedural considerations which can affect admissibility of digital evidence extracted from mobile devices.



THE CHANGING DIGITAL LANDSCAPE SIOSAIA VAIPUNA



PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

WORKING GROUPS



PACIFIC HUB FINDINGS



PACIFIC HUB ACTIONS



JESSAM'S GEE '22



DIGITAL EVIDENCE & MOBILE PHONES MICHAEL CALLAN



PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

JESSAM'S GEE '22



Emma Jaber (Prosecution Team Leader, Organised Crime and National Security, Commonwealth Director of Public Prosecutions) and **Michael Callan** (Technical Specialist, Council of Europe, and CEO, Australian Fraud and Anti-Corruption Academy) then ran a panel, providing practical tips for prosecutors on how to effectively use expert evidence in cybercrime matters. Their tips included when to seek specialist advice, how to recognise this need and the types of electronic evidence that may require explanation from expert witnesses. Each panelist drew on their experience presenting evidence persuasively in court, either as an expert witness or a prosecutor.



WORKING EFFECTIVELY with EXPERT WITNESSES EMMA JABER & MICHAEL CALLAN

BEING an EXPERT WITNESS



slow your CONVERSATION AND KEEP it SIMPLE

CONSTANT COMMUNICATION w- PROSECUTOR IS KEY
 → TIMEFRAME
 → CASE THEORY
 → TYPE of DATA

IMAGINE you'RE EXPLAINING it to NAN.



SIMPLE LANGUAGE the JUDICIARY CAN UNDERSTAND
 DON'T MAKE ANY ASSUMPTIONS of KNOWLEDGE

TAKE your REPORT

BE PREPARED

ONLY ANSWER the Q ASKED
 SHORT + FOCUSED

WHY DO WE NEED EXPERTS?



WRITING REPORTS





FOCUS on FINANCIAL CRIMES CORPORAL SAVENACA SIWATIBAU

IT'S COMPLEX to INVESTIGATE.



IT ALL TAKES TIME

TIMING is EVERYTHING!

IT WILL REQUIRE BOTH ELECTRONIC & TRADITIONAL EVIDENCE



TECHNOLOGY CHANGES FAST... SO WE NEED to UP OUR GAME to KEEP UP

MANAGING VARIOUS HARDWARE, SOFTWARE, JURISDICTION



BUT - IT CAN BE DONE!
WITH PATIENCE & COOPERATION

- FOCUS on WHAT you CAN DO.
- DON'T GET OVERWHELMED by the COMPLEXITY



The final session of the day focussed on financial crimes and key issues with electronic evidence, within the Fijian legislative framework. The discussion emphasised the complexity of investigating financial crimes (particularly scams and identity theft) and

provided some fascinating case studies of financial crimes cases in recent years. This involved hearing again from **Corporal Savenaca Siwatibau** and **Michael Callan**, who were joined by **Razim Buksh** (Director, Fiji Financial Intelligence Unit, Reserve Bank of Fiji).



FOCUS on FINANCIAL CRIMES MICHAEL CALLAN RAZIM BUKSH

THE DEVICE is ONLY A VECTOR: EVIDENCE is the TARGET

ELECTRONIC SYSTEMS as a VECTOR

- INTERNET of THINGS
- FIN. SYSTEMS NOW ELECTRONIC
- TRUSTS & BUSINESSES CAN be SET in SECONDS
- ELECTRONIC PURCHASING and the DARK WEB



IT'S SOPHISTICATED & COMPLEX. IT'S BORDERLESS. NEW PRODUCTS & TECH. IT'S MULTINATIONAL. USE of P SHELL COMPANIES

TIMING IS EVERYTHING! 72hrs

e.g. MONEY LAUNDERING, CREDIT CARD SCAM, LOAN SCAM, ROMANCE SCAM, INVESTMENT SCAM, B.E.C.

FIU: FINANCIAL INTELLIGENCE UNIT
SPECIAL POWERS, inc. ACCOUNT FREEZING

THERE are MANY PLAYERS in the FINANCIAL LANDSCAPE, e.g. REAL ESTATE, ACCOUNTANTS, BANKS, SUPER, BROKERS, STOCK EXCHANGE, MOBILE BANKING, ADVISERS, etc...

*THE PRIVATE SECTOR PLAY an IMPORTANT ROLE in REPORTING

ISSUES with E-EVIDENCE

- VOLATILE & INCONSISTENT
- CLOUD-BASED CRIMINALS
- JURISDICTIONAL ISSUES
- TRAINING AND ENFORCEMENT
- EDUCATION OF JUDICIARY
- COMPLIANCE in FIN. INSTITUTIONS
- GOVERNMENT INACTIVITY
- CORRUPTION

THE WAY FORWARD
HARMONISATION, STANDARDISATION, and CAPACITY BUILDING



DAY 3



The conference-wide discussion following the final session led to participants sharing struggles with policy development, rapidly shifting technological landscapes, as well as practical tips for working with service providers.



WE CAN'T LEGISLATE everything



HOW DO WE MOVE THINGS FORWARD WHEN WE ARE NOT POLICY MAKERS... and THESE MATTERS ARE NOT a PRIORITY for OUR GOVERNMENT?



WE NEED to FOCUS on COMPANY'S TERMS of SERVICE. WORDING MATTERS!

BUILD RELATIONSHIPS WITH THESE COMPANIES.

IT CUTS through GLOBAL LAWS.

DAY 3 END

Day 3 concluded with a buffet dinner at the Hilton Fiji Beach Resort. This was an important time for networking between delegates who hadn't seen one another for many years. As the Chair of PILON, Attorney General of Samoa, **Su'a Hellene Wallwork** provided opening remarks on the importance of a coordinated approach to tackling cybercrime.

Following remarks by **Su'a Hellene Wallwork**, Attorney General of Samoa (above), **Rachel Olutimayin**, Director of Public Prosecutions, Solomon Islands (across) opened the meal.





DAY 4

BRINGING IT ALL TOGETHER

This section of the booklet covers Day 4 Presentations Presentations Bringing it All Together

- **Session 1:** Zyber Panel Discussion on Case Study Outcomes
- **Session 2:** Effective Legislation: Focus on Digital Evidence
- **Session 3:** Case Study in Ransomware
- **Session 4:** Pacific Cyber Stories: Legislation, Electronic Evidence and Prosecutions

Group discussion between law enforcement and lawyers during an interactive session.



BACKGROUND TO SESSION 1: THE COURSES AND PARTICIPANTS

NAME	ROLE	COUNTRY	COHORT
Apolima Tamoā-Panapa	Legal Officer, Office of the Ongoing Government of Tokelau	Tokelau	Lawyers
Betina Ngwele	Principal State Prosecutor	Vanuatu	Lawyers
Davina Nathan	Assistant Attorney-General	Republic of Marshall Islands	Lawyers
Elma Rizzu-Hilly	Coordinator Corruption, Money Laundering and Proceeds of Crime Unit, ODPP	Solomon Islands	Lawyers
Iliganoa Atoa	Assistant Attorney-General – Criminal & Civil	Samoa	Lawyers
Laite Bokini-Ratu	Senior State Counsel, Fiji Independent Commission Against Corruption	Fiji	Lawyers
Mercy Tamate	State Prosecutor, PIC of Family and Sexual Offences Unit	Papua New Guinea	Lawyers
Nixon Alten	Assistant Attorney-General	Federated States of Micronesia	Lawyers
Surely Kamtaura	Legal Officer, Department of Justice and Border Control	Nauru	Lawyers
Tewia Tawita	Deputy DPP	Kiribati	Lawyers
Tupou Kafa Vainikolo	Crown Counsel	Tonga	Lawyers
'Anamaui Maui Langi	Detective Constable	Tonga	Law Enforcement
Aiyaz Ali	Superintendent, Deputy Director of Organised Crime	Fiji	Law Enforcement
Atis Yosef	Inspector, Vanuatu Police Force - Forensics	Vanuatu	Law Enforcement
Colish Jameke	S/C Fraud Squad, Lae	Papua New Guinea	Law Enforcement
Frank Korai	Officer, Forensic Department	Solomon Islands	Law Enforcement
Gabriel Kirby Fakatonu	Constable I/C Digital Forensics Section	Solomon Islands	Law Enforcement
Gasio Rokodolu	Acting Inspector	Fiji	Law Enforcement
Lebuu Gibbons	Lieutenant	Palau	Law Enforcement
Malachi Boinar	F/C RPNGC Forensics	Papua New Guinea	Law Enforcement
Michael Kaierake	Sergeant	Kiribati	Law Enforcement
'Aleksio Tonga	Sergeant	Tonga	Law Enforcement
Me Tuuaga	Constable	Samoa	Law Enforcement
Eli Junior Wilson	Constable	Samoa	Law Enforcement
Terry Sandy	Sergeant - Vanuatu Police Force - Forensics	Vanuatu	Law Enforcement

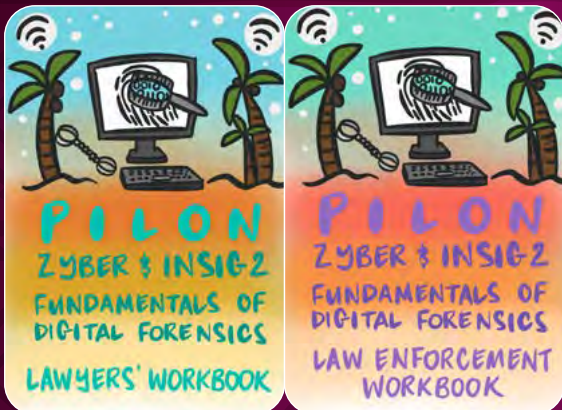
A pre-workshop online training course in 'Fundamentals of Digital Forensics' was delivered to nominated law and justice officials and police officers over 12 weeks from August to November 2022, supported by a workbook and three Zoom case study sessions facilitated by AGD. Nominations were sought from senior officials by AGD and the Australian Federal Police (AFP). Several officers from Pacific police forces and participants in the legal course were subsequently supported to attend the Workshop in-person or virtually.

Participants commented that this training fostered a greater understanding by police and legal participants of their shared challenges when working with digital evidence.

BACKGROUND TO SESSION 1: THE WORKBOOK

The workbooks supplied to course participants covered:

1. summaries of the key concepts from each chapter
2. articles and videos to look at if you're interested
3. a notes section if you'd like to record your questions to ask your classmates
4. further resources from ODPP Solomon Islands and Australian CDPP and procedural examples.



CONTENTS

INTRODUCTION: COURSE INFORMATION	3
Who should use this workbook?	3
When to use the workbook?	3
How is the workbook structured?	3
How can I get involved beyond the course material?	4
How can I get help or more information?	4
Who are the course contacts?	4
CHAPTER 1: INTRODUCTION TO DIGITAL FORENSICS	5
Branches of digital forensics	5
Cybercrime versus cyber security	5
Cyber-enabled versus cyber-dependent crimes	6
Summary of the differences	7
CHAPTER 2: WHAT IS DIGITAL EVIDENCE?	11
What is digital evidence?	11
Where can digital evidence be found?	11
Key concepts in defining sources of digital evidence	12
CDPP practice tips: connecting digital forensics to a person	14
A case study of digital forensics in action	16
CHAPTER 3: THE DIGITAL FORENSIC PROCESS	19
The process based on the ACPO principles	19
The digital forensic process visualised	20
CDPP practice tips: why the digital forensic process matters	21
CHAPTER 4: STANDARD OPERATING PROCEDURE	24
What is a Standard Operating Procedure (SOP)?	24
What are the general features of a SOP?	24
What specific issues can a SOP help ensure?	25
Solomon Islands: Profile of a SOP	26
CHAPTER 5: IDENTIFYING DIGITAL EVIDENCE	29
Identifying digital evidence	29
Examples of devices containing digital evidence	29
CDPP practice tips: when sensitive evidence is identified	30
Cause to seize computers	31
CDPP practice tips: circumstantial digital evidence	31
CHAPTER 6: DIGITAL EVIDENCE PRESERVATION	33
Digital evidence preservation	33
Search warrant	33
Procedures at the crime scene	33
Size and types of storage media	35
CHAPTER 7: ANALYSIS AND DOCUMENTATION	39
What do examiners do in this phase?	39
What kind of questions are answered?	39

How might evidence examination be documented? What does the analysis lead to?	39 39
CHAPTER 8: COMPUTER FORENSICS – INTRODUCTION	42
Defining computer forensics	42
How can a computer be involved in crime?	42
Dead box vs live data forensics	43
Two main rules when coming across a computer	43
CHAPTER 9: MOBILE FORENSICS	50
General principles when collecting mobile forensics	51
Importance of network denial	51
What are some network denial options?	51
Extraction image types	52
Extraction method types	52
Limitations for mobile forensics investigation	53
CHAPTER 10: REPORTING	55
Defining reporting	55
Tool generated reports	55
Written reports	55
Exported files as part of the report	55
FURTHER PILON VIDEOS	58
FURTHER PILON RESOURCES	60
PILON resources on working with other countries on digital evidence	60
PILON resources on combatting online abuse	61
PILON resources on understanding the Pacific response to cybercrime	61
SOLOMON ISLANDS BACKGROUND AND SELF-REFLECTIONS	62
Solomon Islands legislative profile	62
ODPP Solomon Islands' consolidated digital forensics self-reflections	63
CONSOLIDATED CDPP TIPS	65
PROCEDURAL EXAMPLES	68
Digital forensics examination notes	68
Example of a written report	72
CONSOLIDATED GLOSSARY	78

THE CERTIFICATE CEREMONY



During the Workshop, a certificate ceremony was held for graduating participants. During the ceremony, Esther George, the founder and CEO of Zyber, was able to virtually join and provide congratulatory remarks to graduating participants.



ZYBER PANEL DISCUSSION NIXON ALTEN & CONSTABLE GABRIEL KIRBY RONGOLAOL FAKATONU

PROCESS

- PREPARATION
- IDENTIFICATION
- PRESERVATION
- ANALYSIS
- DOCUMENTATION
 - SIMPLE LANGUAGE
 - ENOUGH DETAIL to be ABLE to HAND OVER to ANOTHER
- PRESENTATION

PRESERVATION

DATA MUST BE PRESERVED CORRECTLY or RISK INADMISSIBILITY

WRITE BLOCKING
ANY TOOL that PERMITS READ-ONLY ACCESS

VALIDATION
VERIFYING SOMETHING WORKS AS EXPECTED to.

HASHING
FORENSIC CLONE to PERFORM EXAMINATION

FARADAY BAG
CAN be REPLACED with 4x CHIP PACKETS of ALUMINIUM FOIL

ARSON CAN
METAL CAN MADE of ARSON

PROTECT DEVICE from CONNECTING to NETWORK



PROSECUTION LAW ENFORCEMENT
DIGITAL FORENSICS FUNDAMENTALS

COLLECT, STORE, RETRIEVE, ANALYZE & DOCUMENT ELECTRONIC EVIDENCE



COMPUTER, MOBILE, CLOUD, NETWORK

THE COURSE

DEFINITIONS & PRINCIPLES

IN-DEPTH STUDY:
MOBILE + COMPUTER
FORENSICS

CASE STUDIES
LEARNING APPLICATION

ZOOM SESSIONS
VARIOUS PERSPECTIVES

WEEKLY EMAILS

EXTRA READING

PRACTICAL SESSIONS → SKILLS + TOOLS
BRIDGED KNOWLEDGE GAPS

KEY TAKE AWAYS

FORENSIC TOOLS AVAILABLE

- OPEN SOURCE
- FREE
- COMMERCIAL

IMPORTANCE of CHAIN of CUSTODY

- TRAINING
- LEGISLATION
- SOFTWARE

CHALLENGES

SEARCHING ONLINE
- CONNECTION
- NETWORK RESTRICTIONS

DIRECT COMMUNICATION
- WAIT TIME for RESPONSE

ACCESS to FACILITIES

BALANCING OTHER COMMITMENTS

PACIFIC ISLANDS LAW OFFICERS NETWORK - CYBERCRIME WORKSHOP 2022

JESSAMJ GEE '22



During the Cybercrime Workshop, two course participants (Mr Gabriel Fakatonu, Constable I/C, Digital Forensics Section, Royal Solomon Islands Police Force, and Mr Nixon Alten, Assistant Attorney-General, Federated States of Micronesia) presented during this session on insights gained during the course, as well as an assessment of their own contexts. Each presenter shared recommendations with the audience on building practical skills and working across professions.

Participants then heard provided a presentation on laws of evidence in the Pacific and comment on emerging areas of legal policy focus. By exploring real examples of admissibility issues within evidence law, participants saw the benefits (and unintended consequences) of different drafting approaches.



EFFECTIVE LEGISLATION & DIGITAL EVIDENCE

WHY ADMISSIBILITY MATTERS



GETTING YOUR EVIDENCE THROUGH THE COURT



DETERMINED BY LEGISLATION IN YOUR JURISDICTION



IMPLICATIONS ON TYPES OF EVIDENCE, HELPS TO IDENTIFY GAPS

THEMES and INDICATORS

How is it DEFINED?



DOCUMENTARY EVIDENCE

- SOUNDTRACKS and DEVICES
- FILM/VIDEOS
- TAPES → PHOTOS
- DISKS → DOCUMENTS



BROAD JUDICIAL DISCRETION

- WHAT'S ALLOWED IN
- WHAT'S EXCLUDED
- FLEXIBILITY IN COURT
- REQUIRES LEGISLATION



TARGET CYBERCRIME LEGISLATION

- POSITIVE INDICATOR FOR ADMISSIBILITY

GAPS & UNINTENDED CONSEQUENCES

CASE BY CASE

JUDICIAL DISCRETION ONLY

SPECIFIC CIRCUMSTANCES

EXCLUSIVE PROVISIONS

ONLY OFFENCES "AGAINST ANY OTHER LAW"

UNINTENTIONAL EXCLUSIONS

CASE STUDIES

FACTS FOR CASE STUDY **TWO** (RANSOMWARE)

Dr Tawanda Hondora of the Commonwealth Secretariat took participants through a provocative and thorough case study of a ransomware attack. As a group, participants worked through the legal policy considerations for responding to this crime type, including the necessity of strong legal policy, practice and frameworks for preventing (and prosecuting) future occurrences.

- Country name - Republic of Ngato
- Region – Pacific
- Population – 100,000
- Internet Penetration Rate – 50%
- GDP (2021 est.) – US\$200 million

The Republic of Ngato is a small island country in the Pacific. It used to be part of the Uruna Federation but voted for independence five years ago.

The government has made great strides to improve the country's economy, increase its tax revenue, reduce corruption and foreign exchange leakages, and to significantly reduce its high interest-bearing foreign debts. Ngato is currently rated "BB" and "C" by different credit rating agencies.

On **Monday, 5 December 2022**, the Central Bank is due to facilitate Ngato's payment of US\$10 million to several foreign banks and some vulture funds to service its foreign debt obligations. The government of Ngato is hopeful that this payment will result in a credit rating-upgrade and end the selling-off of its some of its sovereign debt obligations to vulture funds.

8:00AM



Today, Friday, 2 December, at 8AM, most members of staff are struggling to log in to their computers. And those that have managed to log in, find that their computers are extremely slow.

They are also struggling to access some of the bank's systems and files.

1. What kind of cyber attack is taking place?
2. What is at stake for the central bank and the Republic of Ngato?
3. Is a central bank part of a country's Critical National Infrastructure? If no, why? If yes, why? What is Critical National Infrastructure?
4. Do you know whether your country lists the central bank as critical national infrastructure?
5. What should the central bank do in response to this cyber attack?
6. Which key (internal and external) stakeholders does the central bank need to work with to address the challenge?

9:00AM



At 9AM, most of the bank's computers flicker & start to play the song "Breakfast at Tiffany's" and display the following message:

Hi there, bozo!

“ You call yourself a central bank. Well, well, now. We gotcha! We have encrypted all your bank's files and data with the strongest military algorithms R51A40967 and AE S-2356. Your back-up has been encrypted as well. So, don't bother trying to decrypt. All repair tools, including photorec, Rannohecryptor, are useless and will destroy your files, irreversibly.

We will decrypt your data and give you access to your systems **IF you pay US\$1 million in Bitcoin by 12 noon (Ngato time). This is not a joke.** Use this link to receive decrypted samples of your data.

As soon as we get the Bitcoins, you'll get all your decrypted data back. Moreover you will get instructions on how to close the hole in your security and how to avoid such problems in the future. We also know that you are due to pay some big bucks to those grubby bondholders. We too want some of that mula. Sorry! **”**

ATTENTION – If you do not pay US\$1 million in Bitcoin by 12 Noon, the price will go up to US\$3 million. After that we will add a million bucks to every hour that passes without you effecting payment. **ACT NOW OR YOU WILL BE VERY VERY SORRY!**

BTC WALLET – 18TLNdVdZ>mvn/mTVUL3571/wESodhYON1

1. Does the the Republic of Ngato have a National Strategy and Plan of Action for dealing with cyber attacks?
2. Does it need one?
3. Which agency (government or quasi-government) should be responsible for the development and implementation of the same?

9:30AM



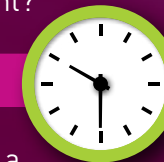
Mr. Jon Tanaka, the governor of the Central Bank of Ngato asks his IT team to work hard to restore services. He asks about back-up servers and networks and timelines.

Mr. Tanaka is informed that the IT team was working hard but this was the first time they had encountered this type of cyber attack and were struggling to get back into their systems. The IT Team has checked the No More Ransom website for keys and applications that can decrypt data locked by different types of ransomware but have not found anything that works ...

The IT also express anxiety about the risk of permanently deleting the bank's data but are continuing to look for solutions. And, although it is not a member, the Governor has asked the Ministry of Information to contact PaCSON (the Pacific Cyber Security Operational Network) and other regional partners. The IT Team undertake to keep the governor informed of developments.

To mitigate against the risk of losing key data as a result of a ransomware attack, what IT policies do you think financial institutions, including central banks, need to adopt and implement?

10:30AM



At 10:30 AM, the governor receives a call from a leading financial journalist, Shirley Basi, who works for the Ngato Financial Daily Newspaper. She is seeking a response to swirling rumours about a ransomware attack on the central bank.

The journalist also wants a response to additional rumours circulating in the past hour about Karoo Investment Bank, which has allegedly sold Ngato government bonds to two vulture funds that are renowned for their aggressive posture.

1. What should the governor/Central Bank do?
2. Is there anything that the Central Bank could have done to stop information leaking to the media?
3. Why do so called vulture funds get a bad name?



11:00AM



11AM The governor sends a text message to the bank's general counsel using his private phone and says:

“ Hey Tom, what do you advise we do here? Should we pay the US\$1 million, get our systems back up and running and ensure that we can make the country's sovereign debt payments on Monday? The greater risk here is a downgrading of our credit rating if we fail to pay on Monday. This will have devastating consequences. Once we are firmly in the clutches of vulture funds, we will struggle to come back up. Also, what's the world come to? Payment by bitcoin. Where and how do we get that? We are a small country we do not do digital currency. Anyway, let me have your views. Jon Bishop” ”

- 1. What advice should the general counsel give the governor? What are the pros and cons of the general counsel advising the governor to: (a) pay the ransomware; and (b) not to pay the ransomware?**
- 2. In your country, are there any statutory/ regulatory rules pertaining to:**
- 3. the advice that inhouse lawyers and external counsel can provide to their clients in such situations; and**
- 4. Whether (a) financial services entities; (b) central banks; (c) government bodies; (d) companies; (e) charitable organisations?, etc. are allowed to pay in response to ransomware demands.**

An intern who joined the central bank two weeks ago approached the Head of IT and informed him that he had used his personal computer to do some research on the dark web and thought that the ransomware message was similar to one that was said to have been used to target a financial institution in the Uruna Federation, the country from which the Republic of Ngato broke away.

The Head of IT shares this information with the governor. The governor is wary since relations between Ngato and Uruna have not been good since the separation five years ago.

But with his options limited, the governor reaches out to his counterpart at the Central Bank of Uruna Federation.

Uruna Federation offers to analyse the encrypted hard drives for the central of bank of Ngato or to send some of their experts over.

- 1. Should the Ngato central bank governor accept the offer? Which offer, if any, and why?**
- 2. And, what factors does the governor need to take into consideration regarding this offer of assistance by the Uruna Federation?**

12:00PM



At 12 noon, the messages of the bank's computers that had not been shut down change to:

“ Ding dong...You have not paid, bozo. The price has gone up. You now need to pay us US\$3 million in bitcoin. End of message. ”

1. Should the central bank engage the cyber criminals?
2. Should the central bank ask for some decrypted files?
3. At what point, if any, should the public be informed of the situation? Should the central bank issue a press release and talk to the media? Who should take such a decision? What factors should be taken into account in taking such a decision? Should there be a policy framework?
4. What are the key legal risks that need to be considered following what is now clearly an escalating situation?

12:10PM



At 12:10PM, governor's personal secretary asks the governor:

“ Does the bank not have insurance to deal with this type of situation? I do not have a PhD nor am I a banker, but I know insurance is important. You know, I have had my fingers burnt enough times and I have insurance even for Jojo, my little darling here. I have insurance for her although I have never needed to claim on it. It's cost me more than I paid for Jojo three years ago. ”

In response, the governor, goes:

“ Ah ha, Lesley. You might have saved my life here. Let me check if we have cyber insurance. ”



- 1. Is cyber insurance a viable option in this scenario?**
- 2. What role would an insurance company play in such a situation?**
- 3. Should cyber insurance be part of measures adopted by organisations that are likely to be attacked through ransomware?**
- 4. How big is the Cyber Insurance Market in the Pacific?**
- 5. If the central bank fails to address this issue and gain access to their systems, what would you say are the costs to the bank and the wider economy?**

9:00PM



Last night at 9PM, the police working together with the intelligence services of Ngato arrested the “intern”. It turns out that he was a spy for the Uruna Federation. The arrest of the “intern” resulted in the central bank being sent decryption keys, which enabled them to resume normal operations in time for normal bank operations on Monday.

- 1. So, would (re)characterise this type of cyber attack? If not, why not? If so, how would you recharacterise it?**



CASE STUDY in RANSOMWARE DR. TAWANDA HONDORA



RANSOMWARE ATTACK SCENARIO

HA HA! WE GOT YOU!
GIVE US \$1m by 12pm.

Do you HAVE INSURANCE?
Does it HELP?
SEEK AGREEMENT
PROTECT SYSTEMS

Should I ACCEPT ASSISTANCE from ANOTHER Gov't?

Should I ENGAGE with the CRIMINALS?

Should I INFORM THE PUBLIC?

* THERE CAN be INTENTIONS OTHER than "REGULAR CRIME"

IT SETS A PRECEDENT
THERE'S NO AGREEMENT/GUARANTEE
MISS the OPPORTUNITY to COORDINATE w- LAW ENFORCEMENT WHO MIGHT HAVE HELPFUL INTEL
* CYBER DIPLOMACY

WHAT DO WE DO? WHO SHOULD WE TELL?

- INTERNAL**
 - CIRT? → IT SECURITY?
 - LEGAL COUNSEL?
 - Comms & PR TEAM?
- EXTERNAL**
 - NATIONAL CERTS?
 - POLICE? → NATIONAL SECURITY?
 - FIUs / AUTHORITIES?
 - GOV'T MINISTRIES?
 - FIN SECTOR AUTHORITIES?
 - COOPERATION ORGANISATIONS?

... MEDIA?? CONTROL the NARRATIVE? PRE-EMPT with INTERNAL Comms?

DO I PAY?

PHISHING? DOoS?

WARFARE... ESPIONAGE? INFRASTRUCTURE? PROPAGANDA? ECONOMIC DISRUPTION?

LEGAL POLICY, PRACTICE & FRAMEWORKS are CRUCIAL.

POTENTIAL COSTS of ATTACK

- 💰 RANSOM
- ⚖️ LEGAL FEES
- 💬 REPUTATION
- 👤 REPEAT ATTACKS
- 📄 INSURANCE COST
- 📁 DATA RECOVERY

Should THERE be a MANDATORY REPORTING FRAMEWORK To COLLECT DATA? ... IT'S DIVISIVE!



PACIFIC CYBER STORIES: LEGISLATION, E-EVIDENCE & PROSECUTION

ATTORNEY GENERAL LINDA S FOLAUMOETU'I, TUPOU K VAINIKOLO RACHEL OLUTIMAYIN

REFLECTIONS from PNG

WHAT DO YOU DO WITHOUT CYBERCRIME LEGISLATION?



FIND a WAY UNDER OTHER LEGISLATION: WIDE + GENERAL PROVISIONS



IMPROVISE. BE INNOVATIVE. USE your INITIATIVE.



MAKE the BEST of the PROVISIONS on ADMISSIBILITY of EVIDENCE in your ACT/LEGISLATION IF IT'S RELIABLE and RELEVANT... Go FOR IT!



PREPARATION!!!



BE PERSUASIVE



BE CONFIDENT BELIEVE in WHAT you'RE DOING. STAND your GROUND.

WE RELY on ELECTRONIC EVIDENCE in ALMOST EVERY CRIME

VIDEO FROM
• CCTV • MOBILES • LAPTOPS
• DESKTOPS • CAMERAS

• VOICE MESSAGES • SOCIAL MEDIA



WE HAVE to BE PRO ACTIVE



HAVE an OPEN MIND

DON'T be INTIMIDATED by the DEFENSE COUNSEL

THINK OUTSIDE the BOX

TONGA'S STORY



ACCENSION to the BUDAPEST CONVENTION

2010 - 2017 ACCEDE!



2016 - START DRAFTING LEGISLATION

5-6yrs TO DRAFT & AMEND LEGISLATION



IT HAS to BE CONTEXTUAL for CULTURE



COMMUNITY GUIDELINES

DON'T ALWAYS ALIGN W- REGIONAL CONTEXT

RELATIONSHIPS! ARE KEY.

ELECTRONIC COMM. ABUSE OFFENCES ACT (1 AUG 2021)

- X BORDER
- CRIMINAL + CIVIL
- POLICE POWERS
- SERVICE PROVIDERS

* NEED to REGULATE the FORM of APPLICATIONS + ORDERS for CIVIL ORDERS



NOT PLATFORM / SERVICE SPECIFIC ... WE CAN BE PREPARED for WHATEVER IS AROUND the CORNER

The final formal session for the Workshop took a closer look at the prosecutor's experience of working on trials involving electronic evidence in Pacific jurisdictions. Our experts shared the challenge of explaining and adducing digital evidence in a courtroom setting, including overcoming the difficulty of explaining technical concepts and common misunderstandings.

FINAL REFLECTIONS



FINAL COMMENTS

HOW CAN WE COORDINATE
a REGIONAL APPROACH
TO ENGAGING SERVICE
PROVIDERS TO ADDRESS
OUR CONCERNS?



IN the MEANTIME... WHAT'S
in the EXISTING
COMMUNITY
GUIDELINES
THAT WE CAN LEVERAGE?



A COLLECTION of
COUNTRIES is MUCH
HARDER to IGNORE.

WE HAVE to BE CLEAR
ON WHAT WE'RE
ASKING FOR



CONNECT
PROSECUTORS
WITH
FRONTLINE
OFFICERS
SO THEY CAN
BETTER
UNDERSTAND
PROVISIONS
& PROCESSES



FINAL REFLECTIONS ATTORNEY GENERAL LINDA S FOLAUMOETU'I

KEY TAKEAWAYS



COMMUNICATION
IS FUNDAMENTAL



DIGITAL TRIAGING
TO REDUCE LOAD



INFORMATION
SHARING



NO COUNTRY, and NO CHILD,
IS IMMUNE.

EDUCATION & AWARENESS are KEY

HYBRID FORMAT

THOUGHTS ON USING A HYBRID FORMAT

“Hybrid workshop is convenient and accommodating for participants of the workshop who are not able to present in person. The contents and participation are amazingly informative and clear despite technical hiccups.”

“I like the fact that virtual attendees participated in group work. That their questions were projected for all and were answered.”

“This PILON meeting is a standard bearer-almost a GOLD standard in how it was done in hybridity. Especially with the graphic artist impressions.”

COUNTRY	REPRESENTING	VIRTUAL PARTICIPANT NAME
American Samoa	Office of the Attorney General	Janelle Etelagi
	Department of Defence	Sophie Harding
		Lauren Wynn
	Attorney General's Department	Matt Jones
	Ashurst (Australia)	Monique Wilks
		Elizabeth Watson
Fiji	Fiji Independent Commission Against Corruption	Inoke Jale
		Mosese Matanisiga
		Frank Tora
		Waisea Jinairavula
		Aporosa Vuinakelo
		Senimili Qolisese
	Fiji Police Service	James Lave
		Samuela Finau
		Gasio Rokodulu
	ODPP	Rukalesi Uce
New Zealand	Ministry of Business, Innovation and Employment	Tracey Amberger
Papua New Guinea	PNG Office of the Public Prosecutor	Linda Shanks
		Elsie Kariko
		Lilly Jack
	Royal Papua New Guinea Constabulary	Sylvester Banibia
		Shaun Kamak
Republic of Marshall Islands	RMI Police Force	Vincent Tani
	Office of the Attorney-General	Cutty Wase
Samoa	Samoa Police Service	Me Tuuaga Polevia
Interpol	Interpol	Wei Xian Tee
		Dong Uk Kim
		Sinziana Hanganu
Solomon Islands	Office of the Director of Public Prosecutions	Elma Veenah Rizzu Hilly
	Director of Public Prosecutions	Margaret Suifa'asia
		Mark Brennan
		John Wesley Zoze
	Royal Solomon Islands Police Force	Frank Korai
		Garnette Kwanairara
Tonga	Tonga Police	Ana Langi
United Kingdom	Commonwealth Secretariat	Emma Beckles
		Shakirudeen Ade Alade
	Zyber Global (United Kingdom)	Esther George
USA	Homeland Security Investigations	Luke Holloway

ANNEXURE 1

COMPLETE WORKSHOP AGENDA

DAY 1 - 29 NOVEMBER

STOCKTAKE OF GLOBAL TRENDS IN CYBERCRIME

Opening Ceremony, Prayer and Virtual Welcome	Attorney-General Linda Folaumoetu'i (Chair of PILON Cybercrime Working Group, Attorney General of Tonga)		
Session 1: Opening Remarks and Keynote Presentation	Ms Tupou'tuah Baravilala (Acting Permanent Secretary of Communications, Fiji)	A Dr Tobias Feakin (Australian Ambassador for Cyber Affairs and Critical Technology)	
Session 2: Recent Trends in Cybercrime and Cyber-Enabled Crime in the Pacific	Mr Wei Xian Tee (Council of Europe/Interpol)	Mr Michael Crowe (Regional Security Advisor, Pacific Islands Forum Secretariat)	Sergeant Titimaea Nemaia (Samoa Police Secondment Member - Pacific Transnational Crime Coordination Center)
Session 2 continued: R Child Exploitation Developments During the Pandemic	AFP National Central Bureau	Dean Chappell, Federal Bureau of Investigations	Damian Rapira-Davies, New Zealand Department of Internal Affairs
Session 3: Cybersecurity & Cyber Expertise - Countering New Threats	Dr Jeffery Garae (Chair, Pacific Cybersecurity Operational Network)	Mr Enoka Feterika (Pacific Islands Chiefs of Police Secretariat, Cyber Safety Pasifika)	Chief Superintendent Kalisi Tohifolau (Tonga Police)
Summary and Close			
Opening Reception	Ms Ana Elefterescu (Senior Project Officer, Council of Europe)	Ms Pirjo-Liisa Heikkila (Head of Political, Trade and Information Section, EU Delegation for the Pacific)	

DAY 2 - 30 NOVEMBER

GENDERED ASPECTS OF CYBERCRIME

Prayer + Review of Day 1			
Session 1: Talanoa - Gendered Impacts of Social Media	Ms Kira Osborne (Pacific Lead, Office of the eSafety Commissioner, Australia)	Ms Tajeshwari Devi (Fiji Online Safety Commission)	Corporal Savenaca Siwatibau (Fiji Police)
Session 2: Pacific Perspectives on Law Reform	Mr Andrew Kelesi (Deputy Director of Public Prosecutions, Solomon Islands)	Ms Josephine Advent Pitmur (Deputy Secretary for Justice Administration, PNG)	
Session 3: Strategies for Supporting Victims of Cybercrime	Chief Superintendent Kalisi Tohifolau (Tonga Police)	Ms Stephanie Chanelle Dunn (Legal Officer, Fiji Women's Crisis Centre)	Ms Lavonne Talei Goundar (Assistant Counsellor Supervisor, Fiji Women's Crisis Centre)
Summary and Close			
PILON Cybercrime Working Group Meeting			

DAY 3 - 1 DECEMBER

OPERATIONAL TOOLS

Prayer + Review of Day 2

Session 1: The Changing Digital Landscape: Safeguarding Pacific Communities in the Evolving Online World

Ms Nicole Matejic (Principal Advisor, Digital Safety, Te Tari Taiwhenua - Department of Internal Affairs)

Mr Jope Tarai (PhD Candidate, Australian National University)

Mr Siosaia Vaipuna (Pacific Hub Director, Global Forum on Cyber Expertise)

Session 2: Digital Evidence and Mobile Phones

Mr Michael Callan (CEO, Australian Fraud and Anti-Corruption Academy, Council of Europe)

Session 3: Working Effectively with Expert Witnesses

Ms Emma Jaber (Prosecution Team Leader Commonwealth Director of Public Prosecutions)

Mr Michael Callan (CEO, Australian Fraud and Anti-Corruption Academy, Council of Europe)

Session 4: Focus on Financial Crimes: Key Issues with Electronic Evidence in the Pacific

Mr Michael Callan (CEO, Australian Fraud and Anti-Corruption Academy, Council of Europe)

Mr Razim Buksh (Director FIU, Reserve Bank of Fiji)

Corporal Savenaca Siwatibau (Fiji Police)

Group Dinner

Attorney General Su'a Hellene Wallwork (PILON Chair, Attorney General of Samoa)

DAY 4 - 2 DECEMBER

BRINGING IT ALL TOGETHER

Prayer + Review of Day 3

Session 1: Zyber Panel Discussion on Case Study Outcomes

Attorney General Linda S Folaumoetu'i (Chair of PILON Cybercrime Working Group, Attorney General of Tonga)

Mr Nixon Alten (Assistant Attorney General, FSM Department of Justice)

Constable Gabriel Kirby Rongolaoi Fakatonu (Digital Forensics Officer-In-Charge, Solomon Islands Royal Police Force)

Session 2: Effective Legislation: Focus on Digital Evidence

Closed session

Session 3: Case Study in Ransomware

Dr Tawanda Hondora (Head of Rule of Law Team, Commonwealth Secretariat)

Session 4: Pacific Cyber Stories: Legislation, Electronic Evidence and Prosecutions

Attorney General Linda S Folaumoetu'i (Chair of PILON Cybercrime Working Group,

Attorney General of Tonga)
Ms Tupou K Vainikolo (Crown Prosecutor, Criminal Division, Attorney General's Office, Tonga)

Ms Rachel Olutimayin (Director of Public Prosecutions, Solomon Islands)

Final Reflections and Closing Remarks

Attorney General Linda S Folaumoetu'i (Chair of PILON Cybercrime Working Group, Attorney General of Tonga)

ANNEXURE 2

IN PERSON PARTICIPANTS

COUNTRY/ORG	REPRESENTING	PARTICIPANT NAME
Australia	Commonwealth Director of Public Prosecutions	Emma Jaber
	Australian National University	Jope Tarai
	Attorney General's Department	Lauren Murray
		Nicholas Wilson
		Sarah Kossatz
	eSafety Commissioner	Kira Osborne
	Department of Foreign Affairs and Trade	Ambassador Tobias Feakin
Malcolm Paterson		
Craig Gillies		
Think In Colour (livescriber)	Jessamy Gee	
Cook Islands	Cook Islands Police	Alan Rua
	Crown Law Office	Jamie Crawford
Fiji	A/Permanent Secretary for Communications	Tupou'tuah Baravilala
	The Pacific Islands Forum Secretariat	Michael Crowe
	Fiji Womens Crisis Centre	Stephanie Dunn
		Lavonne Goundar
	Fiji Online Safety Commission	Tajeshwari Devi
	Office of the Attorney General	Glenys Andrews
		Zanuba Bhatti
Ministry of Defence, National Security and Policing	Savenaca Siwatibau	
Reserve Bank of Fiji	Razim Buksh	
Federated States of Micronesia	Department of Justice	Nixon Alten
		Darrel Poll
Kiribati	High Commission of Kiribati (Fiji)	Annette Tokataake
	Police Service	Michael Bootii
	Attorney General's Office	Benateta Atanteora
	Ministry of Information and Communication Technology	Domingo Kabunare
Terianna Kourabi		
Nauru	Nauru Government	Wenona Deiye
	Office of the Director of Public Prosecutions	Saif Shah
New Zealand	Department of Internal Affairs	Damian Rapira-Davies
		Nicole Matejic

COUNTRY/ORG	REPRESENTING	PARTICIPANT NAME
New Zealand	Pacific Islands Chiefs of Police	Enoka Feterika
Niue	Niue Minister for Natural Resources	Ricky Makani
Palau	Attorney General	Ernestine Rengiil
	Office of the Attorney General	Hila Asanuma
	MoJ (Division of Criminal Investigation)	Lebuu Gibbons
Papua New Guinea	Department of Justice and Attorney General	Josephine Advent Pitmur
	Royal Papua New Guinea Constabulary	Malachi Boinar Colish Jameke
	Office of the Public Prosecutor	Mercy Tamate
Council of Europe	Council of Europe	Michael (Mick) Callan
		Ana Elefterescu
Samoa	Attorney General	Su'a Hellene Wallwork
	Office of the Attorney General	Lolomaivitiiveiuto Faasii Steffany Meredith
	Samoa Police Service	Angelo Chan Mow
	PILON / Office of the Attorney General	Sasae Walter Rosarino Koi
	Pacific Transnational Crime Coordination Centre	Titimaea Nemaia
Solomon Islands	Office of the DPP	Rachel Olutimayin
		Andrew Kelesi
	Royal Solomon Islands Police Force	Michael Bole Gabriel Fakatonu
Tonga	Attorney General	Linda Folaumoetui
	Attorney General's Office	Tupou Vainikolo
	Global Forum on Cyber Expertise	Siosaia F Vaipuna
	Tonga Police	Superintendent Kalisi Tohifolau Aleksio Tonga
United Kingdom	Commonwealth Secretariat	Dr Tawanda Hondora
USA	Federal Bureau of Investigations	Dean Chappell
Vanuatu	PaCSON / CERT Vanuatu	Dr Jeffery Garae

EXTRA PHOTOS





Thank you from the
PILON Secretariat.

