Third Annual PILON Cybercrime Workshop

27 - 31 May 2019, Vanuatu

International Cooperation to Share

Electronic Evidence and Combat Cybercrime

Opening remarks

Justice Taniela Fatiaki, Supreme Court of Vanuatu

GENERAL GREETING

On behalf of the Chief Justice of the Republic of Vanuatu, who unfortunately cannot be here today, I would like to extend a warm and friendly greeting to our esteemed visitors. To the international Delegates, all of the regional participants and speakers. Gud Day Yufala Evriwan Welkom to Vanuatu for the third PILON cybercrime workshop. It is our honour and pleasure to host you all.

AND/ OR GREET KEY INDIVIDUALS:

- Hon. Attorney-General – Mr Arnold Kiel Loughman
- Hon. Minister for Justice – Mr Don Ken MP
- Director General Ministry of Justice and Community Services – Ms Doresday Kenneth
- Your Excellency the Australian Charge d'Affairs Ms Susan Ryle
- Your Excellency the New Zealand High Commissioner – Mr Jonathan Schwass
- Head of the Council of Europe Cybercrime Division – Mr Alexander Seger

I would also like to acknowledge the Government of Vanuatu in supporting this workshop and the Australian Government and the Council of Europe for their continued support to the PILON Cybercrime Network.

INTRODUCTION

Computers, laptops, tablets, and smart phones are part and parcel of our everyday lives. So is the internet and social media. We use them in our homes , in our work places and on the move to great advantage and for the benefit of others; in the legal sector here in Vanuatu , we have the capacity to bring witnesses on outer islands into our courtrooms via an internet cable – this has enormous benefits and cost-saving for court proceedings. Medical professionals can stay in Luganville or Malekula and continue to see patients rather than spend several days travelling or vulnerable witnesses who are unable to travel. Such benefits are unfortunately often matched by the abuse of cyberspace. More and more through the media (and sometimes

in my courtroom) I read and see computers, mobile phones and other electronic devices and digital networks being used to perpetrate frauds, sextortion, harassment, drug trafficking and even terrorism.

The cyber world is so much part of our lives that words such as *"hacking"*, *"cyber warfare", "sexting"* and *"spamming"*, are now part of everyday vocabulary. No longer is *'piggybacking'* a game children play – (it's a method of illegally getting into a computer system) nor, is a *'worm'* a useful creature that lives in the ground. The cyber world like so many other fields of human activity, has its own language and its own domain and it is difficult if not impossible for the ordinary, uninitiated person to penetrate or understand it – that is why ordinary people so often fall prey to those who can use it very effectively.

This workshop starting today has a somewhat lengthy title: ***International Cooperation to Share Electronic Evidence to Combat Cybercrime.*** The agenda has also been designed to build a broad understanding of cybercrime and best practices associated with identifying, collecting, collating, preserving and producing electronic evidence in court from the initial stages of investigations through to the prosecution of cybercrimes.

This workshop comes at an opportune time when our governments, law enforcement agencies and courts are seeing a growing incidence of crimes involving the use of electronic devices such as static ATMs and desk-top computers, and mobile laptops, tablets and smart phones. Almost all fraud committed today involves an electronic banking system, extortion type offences are now committed via texts, email, facebook messenger or dating websites. Indeed, many of the domestic violence offences that comes before our Courts often revolves around electronic text messages as key evidence.

A difficulty here in Vanuatu, common to many of our Pacific neighbours is that almost all of these electronic communications or electronic transactions have an international element: for instance, mobile phone transaction records are held by **Digicel** in Fiji, and banking transactions may originate in or be transacted via Australia or New Zealand – the list of examples keeps growing and we struggle to keep pace.

The Challenge then is to face these issues by introducing appropriate legislation, building our knowledge of these new technologies and developing investigative skills and techniques to deal with this new cyber environment. It is a huge challenge for our small island states with our limited financial and human resources. One thing is fast becoming clear however, and that

is that no one country can cope with the incidents of cybercrime, alone – we need to co-operate if we are to successfully limit and combat it.

For this reason I commend the Pacific Island Legal Officers Network who three years ago started meeting on this very important issue that is affecting all of us every day.

Cooperation

Although cybercrime is borderless, nevertheless, national investigating and prosecuting authorities must respect national borders and each country's sovereignty and territorial integrity. It is vital therefore to put in place measures for co-operation, and information-sharing, as well as investigative assistance and facilitation of evidence-gathering and transfer to reduce and avoid such obstacles in the fight against cybercrime.

This workshop program supports two types of cooperation, namely:

1. In-country cooperation – between law enforcement agencies, the private sector, government and prosecution authorities; **and**

2. International cooperation – between mirror agencies, where information is shared in a manner that is efficient, effective, and legally compliant.

Cooperation requires dialogue or a conversation to start and continue within countries and between countries.

During the practical exercises you will undertake with your colleagues over the next couple of days, that conversation will start for some, and for others, it will be a continuation. Whichever it is, it is very important that each participant fully participates in the dialogue in order to build a personal network of like-minded colleagues and foster a culture of co-operation on cybercrime.

It is encouraging to see in the list of participants, that this dialogue and cooperation is occurring here in Vanuatu at all levels between law enforcement, the private sector, and government and prosecution agencies. The fact that so many of you are here tells me it is also happening throughout the Pacific.

Legislative Reform

There are many challenges for investigators when it comes to cybercrime. For prosecutors and courts however, one of the biggest challenges is dealing with cyber or digital evidence effectively and fairly. At the forefront of addressing such challenges is the enactment of targeted and new legislation to enable us to keep up with this new borderless and formless, highly volatile type of criminal activity where the location of the crime and the criminal almost never co-exists in the same country.

I understand that a new Cybercrime Bill will soon be enacted for Vanuatu that will hopefully close some of the gaps in our legislation and, most importantly, will protect an individual's right to security and privacy as guaranteed under our Constitution. Importantly, I am told this bill will:

- Facilitate the sharing of information and electronic evidence between countries that enact similar legislation. This will enable law enforcement to use it and give prosecution agencies the ability to admit it into evidence in Court in a manner that is fair to both the accused person and the prosecution;

- It will help to streamline court cases and the requirement for expert evidence with the introduction of certificate's as evidence of facts in issue and;

- Ensure evidence is not lost by requiring internet service providers (ISPs) to store communications for a certain period that can be later accessed by law enforcement under warrant.

The challenge for legislative drafters will be, as it is in most countries, to ensure that appropriate checks and balances are put in place to secure an individual's fundamental freedoms as guaranteed by our Constitution.

Without the necessary legislative framework in place, police and prosecutors will be handicapped in the gathering, preservation and production of electronic evidence which has no physical form or fixed location.

Given the unique nature and characteristics of cybercrime, the law and the courts approach to the admissibility and reception of electronic evidence requires a paradigm shift in thinking.

No longer will traditional methods and principles suit. There needs to be more use of legal presumptions regarding the authorship and authenticity of electronic records.

While the prospect of new legislation is encouraging, the fact that these new offences will be investigated and prosecuted in an international context brings a whole new level of legal and practical complexity that needs to be addressed – and that is what this workshop is doing, has done over the past three years and I expect will continue to do into the future.

Close

When the Chief Justice asked me to take his place today I was very happy to do so, as a judicial officer I am seeing the increase in cybercrime and the inability of the law and traditional evidential rules to adequately address it. This is a very important workshop, each of you are key players in your own country's fight against cybercrime and I am confident you will be better placed to make a change for the better when you return.

With those remarks I thank you for your attention and wish you a fruitful workshop and stay in Port Vila.