An Introduction to the Sources of Digital Evidence: How Do Criminal Use Technology?

Me Tawheen Z Choomka and Mr Neel R Purmah

The IJLS organised the course 'An Introduction to the Sources of Digital Evidence: How Do Criminal Use Technology?' on 23 October 2019 delivered by Me Tawheen Z Choomka, Barrister and Secretary Bar Council, and Mr Neel R Purmah, Legal Researcher at the IJLS. Me Choomka and Mr Purmah participated in the Training of Trainers on Cybercrime and Electronic Evidence organised by Global Action on Cybercrime Extended (a joint project of the EU and COE) in August 2019. They are both certified trainers in cybercrime.

This introductory course was necessary because legal professionals play an important role in the investigation and adjudication of individuals or groups that have committed crimes. With the increased number of incidence where these crimes have an element of cybercrime or electronic evidence, there is an increased need for members of the legal profession to be properly trained to understand the nature of these crimes and to also be aware of the applicable legislation. Mr Purmah tackled how computer systems work and their underlying features, and provided examples of the most common illicit activities online. Me Choomka focused on cybercrime from an investigative and evidentiary perspective and made use of practical case studies that lawyers may encounter in their line of work.

Various devices are capable of creating and storing data in digital form and such data may serve as evidence. It is important for law professionals to familiarise themselves with the technical aspects of digital processing systems and networks. Mr Purmah focused on technical features of digital processing systems as well as the types of evidence that can be gleaned from these devices. He then turned to the importance of networks such as the internet and the types of network applications such as email and social networking apps which are considered as crucial in the investigation of cybercrime.

Mr Purmah then highlighted some of the most common illicit activities online. In particular, he warned that Business Email Compromise or BEC - whereby an attacker uses the identity of someone on a corporate network to sent spoofed emails (emails with a forged sender address) and trick the targets into sending money to the attackers' account - is a dimension that has assumed enormous proportions in recent years whereby the losses amount to more than $12 Billion globally.

He also touched upon other common forms of cyber scams online such as ransomware, phishing, SQL Injection, investment schemes, credit card schemes, business opportunities/work at home schemes, 419 frauds, internet banking frauds, disaster charity appeals, herbal viagra, and Russian brides. These scams aim to lure and trick innocent online users into transferring money to a bank account owned by the attacker, to send confidential HR information, or to reveal other sensitive information. Law professionals would skate on dangerously thin ice if they neglect the contingent nature of these scams. This is why it is crucial that they get to grips with the fundamentals of cybercrime in order to be well equipped to advise their clients.

In the second part of the course, Me Choomka focused on the identification of digital evidence in criminal cases; investigation of computer-related offences; and prosecution of computer-related offences. She started by giving some examples of cybercrime such as how cybercriminals allegedly siphoned millions of dollars out of US banks through automated tellers fraud, and an infamous case of software sabotage where Stuxnet disrupted Iran's uranium enrichment programme. Me Choomka then described computer-related offences that are found in the Computer Misuse and Cybercrime Act 2003, ranging from section 3 on unauthorised access to computer data to section 10 on electronic fraud.

Me Choomka then placed emphasis on the definition of electronic evidence as any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a disputed fact in legal proceedings. She highlighted the unique characteristics of electronic evidence, namely that it should be handled by specialists, it is invisible to the untrained eye, it is highly volatile, it may be altered or destroyed through normal use, and that it can be copied without degradation.

Me Choomka also focused on the investigatory procedures that must be followed in the handling of digital evidence. In order to obtain a preservation order, a disclosure order, a production order, power of access, search & seizure, real time collection of traffic data, or a deletion order, an application must be made by the investigatory body to the Judge in Chambers. In relation to the extent of use of data for investigation purposes, Investigation Officers should use data obtained through investigation procedures for the purposes only in accordance with the applicable law and/or in compliance with the order of the Judge, for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offences, assessing or collecting taxes; for the prevention of injury or damage to a person or serious loss or damage to property; or in the public interest. Basic investigation procedures must ensure that the complaints are recorded in details; the victim's

computer system is examined by IT Unit; there is a report and working copy for investigation; application for the preservation order to the Judge in Chambers for an order for the expeditious preservation of data; application for a new order from the Judge in Chambers for Disclosure of Preserved Data (S12) and thereafter a Production Order (S13); and powers of access, search and seizure for the purposes of investigation. Me Choomka ended her intervention on admissibility of electronic evidence and practical case studies.

The course was a huge success inasmuch as it enabled members of the legal profession to get to grips with the fundamentals of cybercrime and electronic evidence. In this era of digital technology, criminals are making use of computer systems to perpetrate all kinds of offences. Knowledge of technology law is thus a prerequisite in the field of investigation and in the prosecution of computer-related offences.