CYBERCRIME INVESTIGATIONS AND PROSECUTIONS: BRIDGING THE GAPS

@

NGERIA COMPUTER SOCIETY'S 26TH NATIONAL CONFERENCE
ABUJA, 19TH – 21ST JULY, 2016

T. GEORGE-MARIA TYENDEZWA, *CFE*

Head, Computer Crime Prosecution Unit,

Department of Public Prosecutions

Federal Ministry of Justice,

OUTLINE

- Interconnected world
- Crimes in an interconnected world
- Legal and institutional framework
- CPPA, 2015 – What Offences?
- Gaps and bridges
- Challenges and Opportunities
- Conclusion

CRIMES IN AN INTERCONNECTED WORLD – RUDE AWAKENING

- All crimes imaginable offline can be committed with the use of computers/ networks either as a target or tool
- Threat to lives and properties, economic sabotage, Disruption of critical services, Terrorism & Propaganda, Theft of information (identity & credit card theft)

- Rude Awakening – 19th February, 2003, a Nigerian Consul in Prague, Czech Republic was shot dead by Jiri Pasovsky, a victim of a get-rich-quick/advance fee fraud (419 scam) who allegedly lost about $500,000 including savings ……

Important Definitions

- **A. Computer crimes**
- 1. Offenses against computer data and systems - Crimes that target computers, networks or devices directly ;
- 2. Offenses related to computers and the Internet - Crimes that are facilitated by/committed through computers, networks
- 3. Other crimes may create digital evidence

- **B. International standards provide a framework for the fight against cyber crime - BUDAPEST CONVENTION**
- . Cyber crime is a worldwide challenge, but ***domestic laws establish cyber crime offenses***
- Computer data: Any representation of facts, information, or concepts in a form suitable for processing in a computer system; this includes electronic and digital information and programs
- DigitalComputer forensics: The analysis of information/data contained within and created with computer systems or devices, using techniques and methodologies to find out what happened, when it happened, how and who was involved.

NIGERIA - LEGAL AND INSTITUTIONAL FRAMEWORK

- **National Cybersecurity Policy And Strategy**

- The need for a holistic National Cybersecurity Policy and Strategy was made apparent by the obstacles that delayed the enactment of cybercrime legislation. Thus, work on developing a National Cybersecurity Policy and Strategy commenced, alongside the efforts to pass the law.
- The national CERT (www.cert.gov.ng)was set up and became operational in 2015. One sectoral CERT (http://cerrt.ng/) is also operational with more sectors to follow.
- The Inter-agency Committee on National Cybersecurity Policy Development finalized a draft policy and strategy in 2014.
- The President approved and launched Nigeria's first National Cybersecurity Policy and Strategy on 05th February, 2015. The Strategy aims to coordinate efforts in the area of cybersecurity and fight against cybercrime, create synergy and promote collaboration between public and private sectors committed to prevent, detect and respond to cybersecurity threats and attacks.

NIGERIA - LEGAL AND INSTITUTIONAL FRAMEWORK

- *National Priorities*
  - **INCIDENT MANAGEMENT & ECOSYSTEM**
  - **NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION**
  - **ASSURANCE & MONITORING**
  - **INTERNATIONAL COMMITMENT**
  - **LEGAL FRAMEWORK**
  - **CYBERSECURITY EXPERTISE & CAPACITY BUILDING**

- **STRATEGIC GOALS**

- Effective legal framework
- Critical Information Infrastructure Protection mechanism
- Cybersecurity assurance

- National CERT management coordination
- Strengthen freedom of information
- Data protection and privacy rights.
- Research and development

- Stakeholder partnerships
- Infusion of cybersecurity culture

- Compliance via Consensus
- Coordinated national awareness
- National cybersecurity manpower
- Strengthen International Cooperation.
- National Cybersecurity Coordination Center (NCCC)

NIGERIA - LEGAL AND INSTITUTIONAL FRAMEWORK

LEGAL FRAMEWORK INITIATIVES		
INTIATIVES		GOALS
Initiative 1	▪ Enactment of Cybercrime Legislation ▪ Cyber Crime Legislation Review Mechanism (CCLR)	i. Operation of Cybercrime Law by year Q3, 2015. ii. Training 50% of Judicial Sector by 2016 iii. Operation of Special Cyber-COP by 2016. iv. Nigeria signing Budapest Convention on Cybercrime and other relevant international treaties by Q4 2016 v. 50% of the Nigerian Public fully aware of operation of the Cybercrime law by Q4 2016
Initiative 2.	▪ Preparation of the Judiciary for Cybercrime Legislations ▪ Capacity building Mechanism for Security & Law Enforcement ▪ Digital forensics laboratories and capacity building	
Initiative 3	▪ International Co-operation Mechanism	
Initiative 4	▪ Public/Private Sector Collaboration Mechanism	
Initiative 5	▪ Legal & Legislative Awareness	
SPECIAL FOCUS		
Data Protection & Privacy **Lawful Interception Strategy**		

THE *CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT, 2015*

- The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 (https://cert.gov.ng/images/uploads/CyberCrime_%28Prohibition%2CPrevention%2Cetc%29_Act%2C_2015.pdf) outlines the legal and institutional frameworks needed to drive/facilitate the nation's preparedness to fight cybercrime. It has made substantive criminal law, procedural law, as well as international cooperation provisions that meet the standards of the Budapest Convention and other international instruments in the fight against cybercrime.

➢ **Part I – General Objectives -** The objects and scope of this Act are to: –

- provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
- Enhance cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, Intellectual property and privacy rights;
- The provisions of this Act shall be enforced by law enforcement agencies in Nigeria to the extent of an agency's statutory powers in relation to similar offences.

THE *CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT, 2015*
WHAT OFFENCES

- Part III – Offences & Penalties (Sections 5 to 36) of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 criminalizes specific computer and computer – related offences and spells out the penalties.
- These include: Unlawful access to a computer; Unauthorized disclosure of access code; Data forgery; Computer fraud; System interference; Misuse of devices; Denial of service; Identity theft and impersonation; Child Pornography, Grooming; Cyberstalking; Unlawful Interception; Cybersquatting; Cyber-terrorism; Failure of Service Providers to Perform certain Duties; Racist and xenophobic Offences; Attempt, conspiracy and abetment; and Corporate Liability.

THE *CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT, 2015*

- PART V - ADMINISTRATION AND ENFORCEMENT
- ***S. 41(2)***

- *"(2) The Attorney – General of the Federation shall strengthen and enhance the existing legal framework to ensure –*
- *(a) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards;*
- *(b) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and*
-
- *(c) effective prosecution of cybercrimes and cyber security matters."*

- ***S. 42 – Cybercrime Advisory Council***

- *Inaugurated on 18th April, 2016 – working to improve coordination, monitoring and evaluation*

THE *CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT, 2015*

➢ PART VII - JURISDICTION AND INTERNATIONAL CO-OPERATION

- Cybercrime and cybersecurity issues are not restricted by geographical boundaries and legal jurisdictions but can only be checked through international cooperation. The issues covered include: Extradition; Mutual Assistance Requests; Expedited preservation of data, Evidence Pursuant to a Request; and Form of Requests

- ***Section 52, Cybercrime (Prohibition, Prevention, Etc.) Act, 2015:-***

" (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.

(2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country."

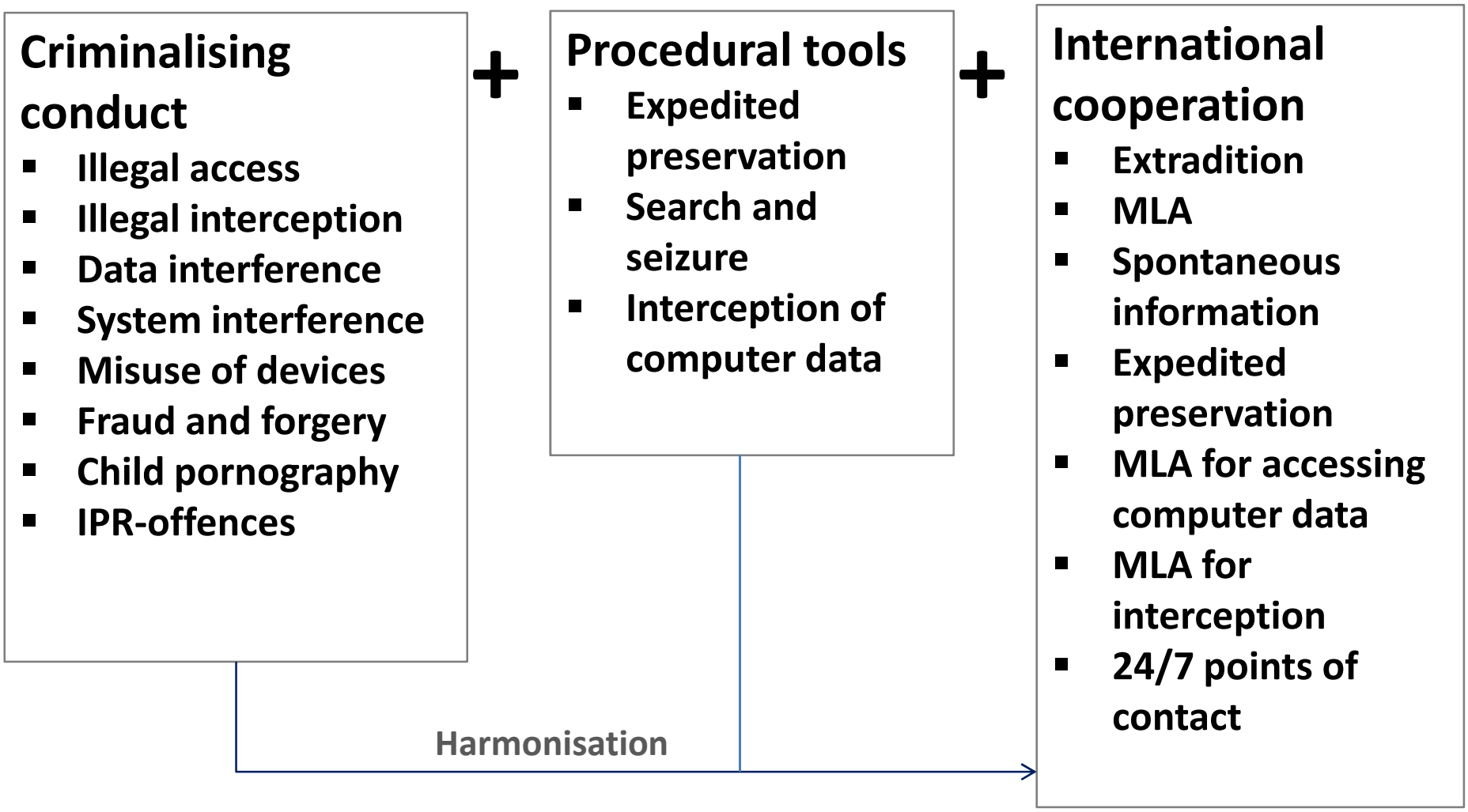
Role of International Cooperation

- Extradition, mutual legal assistance and other types of formal cooperation often require “dual criminality”
- UN GA Resolution:
- “Legal systems should protect the integrity of data and computer systems from impairment and ensure that criminal abuse is penalized””
- Domestic laws have significance across borders

Issues in Collecting and Sharing Evidence

- Will evidence collected in one country be admissible in another country?
- Will computer forensics procedures be accepted?
- Will an MLAT cover electronic evidence?
- Assuming evidence is available

Scope of the Budapest Convention



UNDERSTANDING DIGITAL EVIDENCE

Digital evidence is vital to successful prosecutions in this electronic age

- **Investigators and prosecutors must know:**
- **When is digital evidence important?**
- **Where is digital evidence found?**
- **How is digital evidence collected?**

OBTAINING DIGITAL EVIDENCE - LEGAL ISSUES

More conditions and safeguards as privacy interests increase

- **Content data -The substance, purpose, or meaning of a communication or other data**
- **Traffic data - Data generated by a computer relating to a communication**

- **Subscriber information - Information held by a service provider relating to a subscriber, other than content or traffic data**

Scope of National Procedural Provisions

- Evidence Act, 2011 – Sections 84 and 258 : Admissibility of electronic evidence
- The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 - Section 41
- The Administration of Criminal Justice Act, 2015 – Sections 15(4), 18,37-39, 43 – 44, 106, 143, etc.

Expedited Preservation of Stored Computer Data – S. 38, CPPA

Section 38 (2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency –

(a) preserve, hold or retain any traffic data, subscriber information, non-content information, and content data; or Records retention and protection of data.

(b) release any information required to be kept under subsection (1) of this section.

(3) A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

Expedited Preservation and Partial Disclosure of Traffic Data

Section 55. (1) - Nigeria may be requested to expedite the preservation of electronic device or data stored in a computer system, or network, referring to crimes described under this Act or any other enactment, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data.

Section 55(2) (a) to (f) – spelt out the prerequisites that a request under subsection (1) of this section shall meet.

Production Order – S. 38, CPPA

Section 38 (2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency –

(a) preserve, hold or retain any traffic data, subscriber information, non-content information, and content data; or Records retention and protection of data.

(b) release any information required to be kept under subsection (1) of this section.

(3) A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

Search and Seizure of Stored Computer Data – S.45, CPPA

45. (1) A law enforcement officer may apply ex-parte to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation.

(2) The Judge may issue a warrant authorizing a law enforcement officer to-

(a) enter and search any premises or place if within those premises, place or conveyance –

(i) an offence under this Act is being committed; or

(ii) there is evidence of the commission of an offence under this Act; or

(iii) there is an urgent need to prevent the commission of an offence under this Act

Real Time Collection of Traffic Data –S.39, CPPA

39. Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath;

(a) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement officer to collect or record such data through application of technical means.

Interception of Content Data –S.39, CPPA

39. Where there are reasonable grounds…., a Judge may on the basis of information on oath;

(a) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement officer to collect or record such data through application of technical means.

CHALLENGES AND OPPORTUNITIES

PUTTING THE SUSPECT AT THE COMPUTER (Integrating traditional investigation methods)

- **Electronic evidence may lead to a computer, but not to an *individual***

- Absent direct evidence linking the individual to the crime, look for circumstantial evidence of:
- •Access
- •Knowledge
- •Opportunity
- •Motive
- •State of mind

- **Circumstantial evidence provides the key link between the suspect and the computer**

- **Traditional circumstantial evidence complements electronic evidence in making a stronger case that the suspect was responsible**

GAPS AND BRIDGES

- Data protection – policy & legislation
- Prioritizing evidence
- Understanding Cyber Investigative Roles
  - Investigator
  - Law Enforcement
  - Prosecutor

Digital Forensics – Live Vs Post

Training -

CYBERCRIME DEFENCES

- Using technology to create confusion
- Pointing to absence of direct evidence
- Claiming to lack technical ability
- Suggesting someone else controlled the computer
- Implying that evidence was planted by the authorities

Defence will:

- Attack the collection of electronic evidence, chain of custody, and forensic examination
- Try to impeach the forensic examiner and everyone who touched the evidence

Response

- Prove secure chain of custody for the digital media
- Introduce records showing when the suspect's files were created, accessed, or modified
- Describe in court the devices used to image and record the evidence
- Explain safeguards of the forensic process

Hmm…

- Ideally, cases involving digital evidence should be developed by a team that consists of the prosecutor, lead investigator, and the examiner. Such cases often present special procedural and substantive issues.

- One of the prosecutor's first tasks on being assigned the case is to review the scope of the investigation. Several key issues include:
- A. Preparing and presenting an understandable theory of the case to the trier of fact.
- B. Clarifying the nature of the technological issues.
- 1. Is the digital evidence associated with a "high-technology" crime?
- 2. Although the case might not involve a high-technology crime, is digital evidence nevertheless an important aspect of the case? Or is digital evidence simply involved in the investigation or presentation of the case? (For example, a prosecutor may use a computer simulation or animation to illustrate an expert's testimony.)

TAKEAWAYS / CONCLUSIONS

- Capacity building
  - Investigators/first responders,
  - Digital forensics specialists – analysts and up to date tools
  - Prosecutors, Judges and judicial support staff,
  - Legislators
- Awareness/enlightenment
  - Child online protection initiatives
- Improving international cooperation
  - Networking and knowledge sharing
  - CERTs and CAUs
  - Enhancing regional capabilities – AU, ECOWAS,
  - Other platforms – GPEN, WACAP, CyAN……
- **Engagement premised on the realisation that every country relies on others for assistance in responding to cybercrimes. Every country's ability to fight cybercrime improves when most countries have adequate substantive and procedural laws as well as the ability to share evidence internationally .**
- ***Lastly, an effective criminal justice response to cybercrime thus reinforces cybersecurity*.**

Questions?

THANK YOU.

T. George-Maria TYENDEZWA, CFE
Assistant Director |Head,
Computer Crime Prosecution Unit,
Federal Ministry of Justice, Abuja, Nigeria
E: terlumun.tyendezwa@justice.gov.ng
Alt: tgguno@gmail.com
W: www.justice.gov.ng