



ICT LAWYERS | CONSULTANTS

Legal Instruments Against CYBERCRIME

Basil Udotai Esq.,

Managing Partner, TA

<basil@ta.com.ng> +234-803-306-6004

Africa Regional Conference on
Cybersecurity

Yamousoukro,

November 17-20, 2008

W h o w e a r e

- Technology Advisors (TA) is a young but innovative ICT Law Practice licensed in Nigeria to provide specialty legal services in the ICT fields in Nigeria and within the African Continent;
- Our practice model is centered around 3 key areas: Legal Development; Compliance; and Business Transactions
- TA is peopled by lawyers with considerable knowledge and background in high technology related matters: telecommunication, information technology, and broadcasting; with extensive work experience and international exposure;
- TA is the first and possibly the only law firm in Nigeria focusing exclusively on ICT matters



Nature of ICT

- **Global** – reaches across multiple jurisdictions and legal systems – in defiance of Public International Law (sovereignty) and further complicates Private International Law – applicable law and jurisdiction – liability “forum with substantial impact test”; See the Law of Torts and the “Neighborhood Principle” as a basis for liability!
- **Knowledge based** – proprietary, licensed-based (meaning buyer’s right is limited to use only, with compulsory technical support, conducted not by solutions owners, but by so called Business Partners – management of liability nightmarish); Outright sale of solution is bedeviled by the requirement for 3rd Party Source Code Escrow, with compulsory judicial oversight!
- **Digital/Electronic** – communication and resulting transactions are all electronic in nature as opposed to paper-based materials that current legal systems are familiar with!
- **Fast Paced and Real Time** – communication is fast paced and activities are mostly real time – transactions can complete and evidence lost/deleted very fast – EVIDENTIAL nightmare for law enforcement

N a t u r e o f I C T

- **Inherently Insecure** – No such thing as a Secure system or network; Internet was not built as a SECURE platform but on open standard;
Global Standard of **Interoperability** for systems and devices;
- **Mired by Legal Externalities** - 3rd Party Devices; unknown Intermediaries; making Outsourcing unavoidable – issues with PRIVACY ;
- **Anonymous** – issue with Identity Theft; I can be you, your wife, your Pastor or your President
- **Unlimited Scalability** – 40m credit cards stolen from the Mastercard™ Processing Center, Arizona, USA last year; recently DSW Shoe Warehouse
- **Fiercely Competitive** - Leading to enticing freebies with all sorts of complicated strings attached – issues with Privacy; Google v USA; Yahoo v Republic Of China; AOL India!
- **Cheaper Communication** – all night browsing – “everyday is for the owner, one day for the THIEF!” Mirroring and scanning of networks for **access points and code breaking cheaper;**

N a t u r e o f I C T

- **Ever changing** – “All computers to communicate and all communication gadgets to compute!” INTEL. Add Broadcasting (NetTV; iPod and 3G phones) then we are all in trouble – in terms of regulation, law enforcement and legal remedies! **CONVERGENCE!** New technology media and devices are being introduced regularly that confounds legal systems and judicial procedures – **iPhone is not just a phone**, its also an MP3, its also a Broadcast media as well as Internet platform for data services!
- Still operates in the physical – **eFraudster** lives amongst us **NOT in the Internet!** Issue with Apprehension and criminal charge – **ATTRIBUTION!**
- **Value-neutral** – the Good, the Bad and the Ugly!!!
- **It's a Shared System!** – what affects Cote diVoire affects Nigeria and can also affect America affects – this is the basis for global cybersecurity assistance.

CASE 1

Nigeria v Fasade Tomide (AKA Mike Cole)

- **Facts of the Case:** Around March 2004, tractor parts valued at \$31,000 USD was purchased with fraudulent credit card by one Mike Cole of Mushin, Lagos. A complaint was filed with the FBI by Thill Track and Tractor Services, Inc. When a 2nd order for parts valued at \$12,000 USD was placed by the same Mike Cole, it was tracked by the FBI in cooperation with EFCC. Accused was arrested after paying for the delivery and accepting the goods. He was charged with receiving goods by False Pretences; Conspiracy to receive goods by false pretences; and/or Attempt to receive goods by false pretences. Accused confessed to placing orders but retracted in court.

CASE 1

Nigeria v Fasade Tomide (AKA Mike Cole)

- **Issues for Determination:** “That there was a pretense, that the pretence emanated from the accused, that the said pretence was false, that the accused person knew of the falsity or did not believe in its truth, that there is an intention to defraud, that the thing is capable of stolen and that the accused person induced the owner to transfer his whole interest in the property”
- **Defence:** Prosecution failed to prove that the document containing false pretence emanated from the accused; the fact that he received the parcel in question without more was not sufficient to prove the necessary ingredient otherwise the court would be speculating... Evidence of receipt of parcel without proof of intention to defraud is insufficient.

CASE 1

Nigeria v Fasade Tomide (AKA Mike Cole)

Court Decision:

- No one tendered any evidence of a representation from the accused, which is false and which forms the basis of the deception upon which the company acted and forwarded the goods. “Communications on the Internet are tangible, sufficiently traceable and could be reproduced and tendered in court... No details of the fake credit card used for ordering the goods was tendered, no record of the Internet transaction that led to the fraud was tendered.”
- The berated the Prosecution’s reliance on the accused confession as symptomatic of a systemic deficiency in forensic investigations... a deficiency further endangered by the ignorance of the investigators of developments in case law, which has set limitations on such assumptions.
- In conclusion, the court held that the prosecution had failed to prove each of the counts of offences alleged against the accused person, beyond all reasonable doubt. It therefore had no choice but to discharge and acquit the accused accordingly.

Case 2

Punch Newspaper Website Hacking

- The website of the Punch Newspaper in Nigeria was taken over by a group who identified itself as **Ukrainian HACKERS** for several days – fall in readership and decline in advertisement; issues with **TRUST** of content;
- The newspaper had no law enforcement assistance, case was treated as a private matter, seeming **cross border** nature of incident compounded matter;

Case 3

News Agency of Nigeria (NAN) - eMail Prank

- An Email prank at Nigeria's major news house – the News Agency of Nigerian (NAN), led to a **national embarrassment** causing several arrests and a closure and suspension of operating license of a major TV Station – Channels Television;
- Treated as a Treasonable act, investigations and arrests by the SSS – **old law over new crimes**;

Case 4

Is this Cybercrime? What law applies?

- Customers on a major operator's network could not load recharge card due to **network issues**. RESULT - A naval officer stabbed his neighbor, **a recharge card vendor**, to death thinking the vendor sold him a fake recharge card;
- Any legal liability on the operator?
- Any extenuating circumstances for the Offender?
- Which law applies here? Criminal law of murder? Communication Law on quality of

Legal Requirements

- A . S u b s t a n t i v e P r o v i s i o n s ;
- B . P r o c e d u r a l P r o v i s i o n s ;
- C . E n f o r c e m e n t R e s p o n s i b i l i t y – a l l
e x i s t i n g l a w e n f o r c e m e n t a g e n c i e s o n t h e
b a s i s o f s t a t u t o r y a u t h o r i t y ;
- D . P r o s e c u t o r i a l A u t h o r i t y ;
- E . I n t e r n a t i o n a l L a w E n f o r c e m e n t
C o o p e r a t i o n

Legal Example – Nigerian Draft Law

Offences & Enforcement

- **Enforcement of the Act by Law Enforcement Agencies**
- **Unlawful access to a computer**
- **Unauthorized disclosure of access code**
- **Fraudulent electronic mail messages**
- **Data forgery**
- **Computer fraud**
- **System interference**
- **Misuse of devices**
- **Denial of service**
- **Identity theft and impersonation**
- **Records retention and data protection**
- **Unlawful Interception**
- **Failure of service provider to perform certain duties**
- **Cybersquatting**
- **Cyber-terrorism**
- **Violation of intellectual property rights with the use of a computer, etc**
- **Using any computer for unlawful sexual purposes etc**
- **Attempt, conspiracy and abetment**

Nigerian Draft Law

Part II – CIIP

- **SECURITY AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE**
- Critical information infrastructure, etc.
- Audit and inspection of critical information infrastructure.
- Offences against critical information infrastructure.
- **Civil liability**

Nigerian Draft Law

Part III – General Provisions

- Jurisdiction, etc.
- Powers of search and arrest.
- Obstruction.
- Admissibility and evidentiary weight of electronic documents
- Tampering with computer evidence.
- Prosecution.
- Forfeiture of assets, etc.
- Compounding of offence.
- Order for payment of compensation, etc.
- Conviction for alternate offence.
- Power to make Regulations
- Interpretation
- Short title

Capacity Building & Awareness

- Institutional Capacity Building:
- A. **Enforcement** – Police Cybercrime Unit;
- B. **Prosecution** – Computer Crime Prosecution Unit (CCPU) for the Office of the Attorney General
- C. **Judiciary** – Digital Evidence Management System and Judicial Reform Project, focusing on new Court Rules and Training of officials for Electronic Evidence Handling
- D. **Public Private Collaboration (PPP)** – CERT – National Capability for computer emergency responses and incident handling – issues: One size fit all (joint)?, or separate for industry and Government;
- Awareness Programs: 3 pronged approach: institutional, sectoral and general public enlightenment

Global Cooperation

- **International Law Enforcement Cooperation** – provide adequate capacity (technical facilities and human skill) to enable cross-border information exchanges and joint LEA operations (MLAT no longer serves the purpose in view of speed and potential for multiple “forum shopping” by cybercriminals before hitting target.
- G8 24/7 Network; Council of Europe’s Convention on Cybercrime; European initiative, open to all countries, currently 40 countries, including USA, Canada, South Africa and Japan. Nigeria is not a signatory member, but represented in the 24/7 Network

Conclusion

Cybersecurity is about **technology, people and processes**. A great part of the process is Legal Process. Unless a well crafted law is put in place, with an effective enforcement mechanism, the people and the technology elements of cybersecurity would lack the control required to foster cybersecurity and enforce cybercrime.

A good law is one that takes account of the unique character of the underlying technologies; the propensity of people to manipulate the system; and the cross-border nature of ICT services.

THANK YOU



2nd Floor, Oakland Center,
Plot 2940, Aguyi Ironsi Street, Maitama, Abuja, NIGERIA
Tel: +234-9-870-8979 info@ta.com.ng www.ta.com.ng