Lex Informatica 2012 – Cyberlaw @SA 3 , Clouds, Forensics and Security – how secured are you ?

The much anticipated Cyber law conference by Lex Informatica and Snail Attorneys at Law took place on the 1st and 2nd October at the FNB Conference Centre in Sandton. The seminar, which was packaged along with a book launch – "**Cyberlaw@SA III"**, edited by Sylvia Papadopoulos and Sizwe Snail, comprised experts and specialists on Cyber Law and Cyber Forensics.

Domain Name Disputes

Inaugurated by the host, Attorney Sizwe Snail, "**Domain Name Disputes"** was the opening topic to set the conference in motion. As this is also a highly contested argument between domain users, Snail described the domain name as a common, yet exclusive means of one to infringe or exploit other trading names or trade mark, and simply by adding "....the said name after the 'www'. In South Africa people usually registered their businesses under either .com or .co.za to operate in South Africa and International spheres".

Adding to that, the Pretoria attorney gave a reference of 2006 regulations in terms of (s) 69 with (s) 94 of the Electronic Communications and Transactions Act 25 of 2002 drafted on concepts of abusive and offensive registrations defined according to dispute resolution process. (Also see www.domaindisputes.co.za). In 2007 the South African Institute of Intellectual Property (SAPIIL) was accredited as a service provider, initially for a period of two years, to provide alternative dispute resolution (ADR) servicesHe went through the legal process (procedure), the grounds for filing a complaint, the factors that indicate whether a registered domain name is abusive or offensive and the relevant defences.

To institute a domain name disputehe demonstrated how one should access the Domain Disputes website, which provided a 'one-stop shop' where one can bring a dispute, have it adjudicated and, once adjudicated have the decision published on the website and enforced by ZADNA.

He added that the price of instituting a domain name dispute is a non-refundable R 10 000 if it is by a single adjudicator and R24 000 by three adjudicators if you believe that your matter is a serious one or would require a panel of three independent thinkers He thenspoke about the ADR process and the grounds for filing a dispute.

Mr Snail said that domain names usually uses a 'first-come-first-serve' principle with regard to the 1st time registration of a domain name unless a person can show that he has prior rights to the registrant doman name registration or can rely on the common law passing off remedy or Trade Mark Act remedies.

In the case of ZA2008-0020Mixit v Andre steyn it was held that , "a complainant only have to show rights in a name that is similar to the disputed domain name on the date of the dispute and not on the date upon which the domain name was registerd "

AttoneysSnail said that the ADR regulations make provision for a domain name complaint to be instituted where the registration of a domain name –

- takes unfair advantage of the rights of a trade mark owner;
- is contrary to law;
- gives offence to any class of persons;
- amounts to hate speech, racism or could be considered contrary to public policy.

Mr Snail provided an example of unfair advantage by citing a case involving football association Fifa. In the case ZA2007-0007 Fédération Internationale de Football Association (FIFA)v X Yin, Fifa had a website 'fifa.com' but had not registered 'fifa.co.za'. A South African registered 'fifa.co.za' in his own name and tried to sell it to Fifa.Mr Snail said that FIFA won the case because the website the registrant had registered was identical to

the trademark which FIFAhad registered. He said that the burden of proof shifted to the registrant as he had to show that the domain name was not an abusive registration.

Mr Snail said that the court took into account that FIFAa was the worldwide governing body of soccer and organised and managed the international soccer tournament officially called Fifa, was the registered holder of numerous registered trade marks consisting of or incorporating the word FIFa in South Africa and internationally.

Mr Snail said an abusive registration was where a domain name was registered in a manner which took unfair advantage of, or was unfairly detrimental to the complainant's rights or has been used in a manner that takes unfair advantage of, or is unfairly detrimental to the complainant's rights such as in the decisions of ZA 2007-0003 -Telkom SA Limited v.Cool Ideas1290 CC , ZA2011-0064 MR. MAX DU PREEZ vs. PRAAG - DANIEL ROODT, and ZA2008-0014 AUTOMOBILES CITROEN vs. MARK GARROD

He added an offensive one is a domain name which is contrary to law.

Mr Snail added that factors that indicate that a registration is not abusive or offensive include where the registrant has used or made demonstrable preparation to use the domain name in connection to a good faith offering of goods and/or services;(see the case of ZA2007-0005 Telkom SA Limited and TDS Directory Operations (Pty) v.The Internet Corporation). The registrant may be excused of an abusive registration if, before he becomes aware of the complaint's cause of action, he had already done certain things including actually using the name in connection with a good faith offering of goods or services. (see decision of D2005-0472 Hexagon v. Xspect Solutions Inc) where " failure to make bona fide use of a domain name during a two-year period following registration constitutes bad faith. Another defence is when the registrant has been commonly known by the name or connected with a mark that is identical (see ZA2007-0001 MR. PLASTIC CC vs. MR. PLASTIC & MINING PROMOTIONAL GOODS) or similar to that of the domain name and when the domain has fair comment and/or fair criticism. (see the Constitutional Court decision of Laugh It Off Promotions CC v South African Breweries International (242/2003) [2004] ZASCA 76; [2004] 4 All SA 151 (SCA).

Another defence would be where the registrant has commonly been known by the name, or has made legitimate non-commercial or fair use of the domain name.(see the decision of ZA2007-0001 Mr Plastic Mining and Promotional Goods v. Mr Plastic cc). He may also defend the complaint if the domain name is used generically or in a descriptive manner

and the registrant is making fair use of it or if it is used as fair criticism of a person or business. (ibid)

Mr Snail said that an arbitrator –

- can refuse a dispute ;
- may transfer the domain name; or
- may make a settlement agreement an Ruling ;

Mr Snail concluded by saying that either of the parties can refer the matter to the High Court at any time for determination, appeal or review adding that he has never heard of a dispute where a party went to court. The dispute registration can be filled electronically, via e-mail, posted, faxed or couriered.

Clouds and Forensics and Cyber Crime

Arun Kumar, in a 2011 article titled Cloud Forensics – The Introduction, explains cloud forensics as back-up servers and these could be used by investigators to reconstruct crime for investigation while business is carried out using main servers. Michael Kohn, Manager of Cyber Security and Risk Advisory at Deloitte, drummed on the **Cloud Forensics** – cloud computing and cloud storage. Cloud forensics Kohn emphasised the need for growth in that feature and further educated the audience on a few examples of cloud computing,

and how one's everyday social networking sites such as Facebook, LinkedIn, WhatsApp and Twitter to name a few; as part of cloud computing and everything else was stored in cyber....much as it could be "deleted" off one's system.

"Before one could use a cloud computing service, they should establish its security measure requirements and whether is it safe. One must ask how and where would their data be stored, and who else might have access to it," Kohn advised.

From the Department of Criminal Law and Procedure at the University of Johannesburg, was Professor Murdoch Watney, who spoke on the **Cyber Crime Regulation**. She began by discerning between Cyberspace and the Internet, saying that these are often mistaken for synonyms, while there was actually a difference. She said whilst the Internet was commercial and developed in the U.S, a big change in cyber law should be regulated in the future. Alluding to the usage of internet penetration, she said 20% internet users in South Africa fell heavily on mobile access through their phones also sighting that a big chunk of those users did not own computers.... "Perhaps that's a nag banks and shops with online services should consider.

"Much as there is significant positive growth in the penetration of the internet, the downside is cyber crime," she continued. Prevention, she says; should be the first and foremost measure of security in order to detect cyber crime as soon as possible. Main concerns of this cyber crime concerns was business and government, who have found themselves prone to and as targets of cyber crime.

Prof. Watney ripped more into the economy and cyber crime issue almost as "one joint to the hip". Cyber crime she hints, had transformed into a bogus economy on its own, running parallel to the mainstream financial market. "It's normally conducted by syndicates and sophisticated crime groups that normally know how to cover their tracks," she further said before adding that should the South African economy find stability, then the cyber crimes could be lessened or prevented in many instances.

Another point Professor Watney drove to in terms of a "thin line between cyber crimes and physical offences", was the streamlining or common joining point such as in the case of Thabo Bester – the convicted "Facebook" rapist and murderer. "In this instance, Bester's crimes were physical and not cyber, but then the two mediums were beginning to wedge a thin line between the two."

Computer Forensics and E-commerce

Jaco Swanepoel, a Computer Forensics Analyst from the Cynae (Computer Forensic Laboratory) gave his talk on the subject he defined as analysing and collating of computer data that could be presented before court and also used as evidence. Swanepoel's types of cases involved e-mail misuse, fraud and recovery of deleted data, i.e. downloaded information as well as search engines' traffic.

"In that manner, companies are able to examine how their employees spend their time at work. We also look at file metadata and see the programmes run on it and when last were they run," he said.

The E-commerce subject was handled by the Professor Tana Pistorius from the UNISA, who opened Day Two of the conference. Hers was about the internal and external

alignment of South African e-commerce law. “Legislation alignment was essential for legal certainty and protection of individuals...”

She gave two key principles in aligning e-commerce laws, i.e. Functional Equivalence (translation of requirements from print to electronic) and Technology Neutrality (flexibility of technology to accommodate future technological innovations).

She referred to the Companies Act 71 of 2008 as complete alignment with the Electronic Communications and Transactions (ECT) Act in line with the meaning of electronic communication but on the other hand, said the Consumer Protection Act 68 of 2008 contained a different definition.

E-courts in Brazil , Online Defamation and POPI v FICA

Then entered one of the International speakers at the conference, Professor Claudio S. de Lucena – the Dean and Professor of Law at the Paraiba State University in Brazil, and his speech was on the Brazil’s strides on cyber law. Professor Lucena told the conference on the **Development of E-courts** in Brazil and how successful they have been in their existence.

“E-courts in Brazil run throughout the clock and practitioners are able to access courts from wherever they are and at whatever time,” he said. He also showed slides and pictures of the order and filing system used in Brazil and how effective the e-court system was. With that as a backdrop, Professor Lucena said lawsuits in Brazil happen both online and on the internet and that digital copies are rendered as originals. Not only in exchange of documents, but also in the entire process of a lawsuit, even though there were concerns on the speeding of outcomes and sentencing.

Professor Sanette Nel, also from UNISA tackled the question of **Online Defamation**. Her examples were on defamation and liability on single or multiple publication rule. “Single publication rule did not allow multiple defamation suits to arise from a single defamatory statement that is published multiple times, while the multiple publication rule states that each publication of defamatory material gives rise to a separate cause of action,” she clarified.

Professor David Taylor of Law and Information

Technology and Law Consultant, tore into the **Protection of Personal Information Bill – POPI** (B9 of 2009) against the **Financial Intelligence Centre Act 38 of 2001 (FICA)**. The subject was on the theme: **The practice of privacy and anti-money laundering for global companies and their South African subsidiaries**;

“Secrecy laws shouldn’t prohibit sharing of information by financial institutions, adding that anti-money laundering measures require certain disclosures of customer information, data and documents,” Taylor said.

In the clashing of this Bill and Act, Taylor explained by saying that while the introduction to the POPI recognises the right to privacy in (s) 14 of the Constitution, the right bears the right to protection against unlawful collection, dissemination and retention and use of personal information and that the state must respect, protect and promote the rights in the Bill of Rights.

But then again Professor Taylor said FICA says any quarrel relating to matters dealt with in the Act, save for the Constitution, the provisions of it prevail. However, he noted that POPI had yet to exist in the passing of FICA.

IT Security Management

The last speaker of the conference was Conrade Pasiya of Conipas International Management Solutions. Pasiya spoke on **IT Security Management Systems** and how important it was for companies to secure their data. He warned of the detrimental effects cyber crime could have on companies and business, given the malfunctioning of information technology and susceptibility and breakdown of security systems.

“Ensuring cyber security, enforcing rights and protecting critical information infrastructures required major efforts by the state both at national level and in cooperation with international partners,” Pasiya added.Payisa also got stuck into the importance of company information security measures. From the printer one might render defunct, to the documents/paper an employee might have forgotten to shred, all those are part of company data security measures and Payisa drove a lesson in to close the 2012 Cyberlaw Conference.

This press release was compiled by Mpho Dhlamini for Blackwall Multimedia and pictures used Courtesy of Nomfundo Manyathi (De Rebus).

Contact:

Info@blackwallmultimedia.co.za and www.blackwallmultimedia.co.za

OR

Contact Snail Attorneys directly at Ssnail@snailattorneys.com or +27 83 477 4377