Cyber Security & IP – A Cautionary Tale

N. S. Nappinai
Advocate
nappinai@nappinai.com
Founder Member – Technology Law Forum

Roadmap

- Courts as Consumers: From Procurement to Implementation
- Courts as victims - Smart Courts Smarter criminals?
- Courts as Critical National Infrastructure / Protected System – Threats & Concerns

IP & Open Source

- FOSS: Free & Open Source Software;
- Free – Freedom and not free of payment;
- Copyleft Concept – Statutory to Contractual General Public License (GPL) – just one of many contracts binding open source use;
- Taint or virus of Open Source;
- Pitfalls? Easy to breach or openness its protection?

Not so Ximple

- 2015: Ximpleware, Inc. Vs. Versata Software, Inc. (US)
  - Alleged violation of GPL V.2 by Versata;
  - Versata customers sued for alleged violation of GPL terms;
  - Court rejected domino effect and held that customers use not tainted by Versata's violation;
  - "One tier" structure: violation by distributor held to not violate "downstream" licensees;
  - Violation came to the fore from Versata Vs. Ameriprice discovery process when latter found use of Open Source software in Versata's financial services software!

Copyright or Contract?

- *Jacobsen Vs. Katzer:*

- Held: infringement if breach of OSS is of a "condition," or a term that "limits the scope" of the license;

- If its of a "covenant" or a promise for grant of license, its only a breach of a contract;

Patents Vs. Copyrights

- Ximpleware Vs. Versato:
- Ximpleware claimed breach of patent rights;
- Held Ximpleware's argument amounted to "bait & switch";
- GPL download amounts to implied estoppel / license to use patent also;
- Held that Company cannot give Copyright license on one hand and claim patent violation on the other;

Little Kernels

- 2015: Germany: Linux sues VMware
- Alleged violation of GPL v.2 terms in "vmkernel";
- Kernel, a blend of proprietary software and OSS;
- Source code not disclosed under GPL V.2;
- Issues pending decision is on extent of derivative IP when OSS is used;

Google's Googly

- May 2016: US: Oracle Vs. Google ($10 Billion Suit)
  - San Francisco jury holds in favour of Google!
  - Held reuse of Java's core software interfaces in mobile operating system was fair use;
  - Royalties of billions saved!
- 2011: Bedrock Computer Technologies, LLC, Vs. Google: $ 5 Mil over Patent violation;

Courts As Victims

- **Smart Courts & Smarter Criminals**

Immunity?

"There are two kinds of organizations: Those who have been hacked and those who will be."

Kaffenberger, Lincoln (2015)

Power Play!

- 2015: Ukranian Power Grid Hack:
- It all began with a Ghost Story – almost…..
- 30 power stations down in a matter of

seconds;

- Data Obtained through Spear-phishing;
- Multi-pronged attack!
  - substations down through hack;
  - Operators incapacitated by uninterrupted power supply being reconfigured (deleting, destroying or altering code);
  - DDOS to take down telephone lines;

tick, tick, ticking…

- June 2016: Plymouth Youth Court convicts teenager;
  - 16 year old admits to cyber attacks on "websites across the world including Devon and Cornwall Police and Seaworld"; (http://www.itv.com/news/westcountry/2016-06-28/teen-admits-cyber-attacks-on-worldwide-websites/)
  - Denies 2 counts of: Tweets of "Sorry gentlemen, the clock is ticking" – sent to American Airlines & Delta Airlines;
  - Former tweet tagged to the White House Twitter;
- 2013: Miami, Florida: Turner Guilford Knight Correctional Center breached: All cell doors of maximum-security wing opened simultaneously. Prisoners set free;

Data & Leaks – Panama Papers

- 2016: The Innocuous Email hacked!
- Insider Threats & Whistleblowers;
- Beware the Disgruntled Employees – the Weakest Link!
- Vulnerabilities in outdated software used;
- Emails not “encrypted”!
- Data leaked to German Journo;
- Global Cooperation – 107 Journalists from 80 Countries work on segregating the mega data (2.6 Terra bytes)!

Wailing the Talk

- 2015: Talk Talk No more!
- Century + hit on Customer data loss
- 60 m pounds lighter;
- Reason? Hack the ISP to mine more data!

Innocent till you are Caught!

- 2015: Ashley Madison:
- The Extra-Marital Hack!
- Impact Team & Moral Policing!
- 25 Gigabytes of data breached!
- Damned if you do
- Damned if you don't?
- Liability in the face of libel;

Target targeted

- 2013: Target the Departmental Store is targeted for a super – hack;
- Entry through network credentials stolen from refrigeration service providers;
- Malware introduced to cash registers between thanksgiving to Black Friday to steal card details – tested and then launched!;
- Within 2 days, malware in all

"point of sale" devices;

- Live-streaming of card details!

Troubled Waters

- **March 22, 2016:** US – Attackers Alter Water Treatment Systems;
- Water flow and the quantity of chemicals being added to the water to treat it modified;
- Poor security architecture; high risk vulnerabilities exploited; Outdated operating systems blamed;
- **March 2016:** US: Iranian hackers convicted for attacks on 46 financial institutions and a New York Dam;

Ransomware

- Data as a Weapon; Encryption – the tool;
- 2015: Cryptowall: USD $500 to unlock files;
- US places loss at USD $ 325 Million!
- Cryptolocker - the Menace:
- $17,000 paid by Hollywood Presbyterian
- Ransomeware at Indian Shores!

Inadvertent Insider Threats

- *"Given the choice of dancing pigs and security, users will choose dancing pigs every single time. (*McGraw, G. and Felten, E., 1998)

Uphill Task

- May 11 2016: Capitol Hill under attack:
- Hackers infiltrate congressional computers, encrypt their contents, and then force users to pay a ransom to get their access back;
- Emails hacked & malware circulated through recognizable mail ids;
- Staffers inadvertently download malware when they open link in email;
- Malware encrypts all files on that computer, including shared files, making them unusable until a ‘ransom’ is paid;
- With Congress being the target, hopes for remedy for ransomware!

Go Phish!

- 2011: McAfee discovered a 5 year breach "Operation Shady Rat" stealing data from over 70 Government and corporate agencies, including 8 State and County governments;
- Entry point? Infected emails sent to employees, who unintentionally downloaded attachments;
- Attachments? Images (including of suggestive pics of woman in a Hat!) – Steganography;
- Spear-phishing: Targets in courts: judges, administrators, and elected officials;

Enemy at the Water Cooler

Contos, B. T. (2006)

- M/s. Planet Edu Private Limited Vs. Vishal Mehta: Punjab & Haryana High Court:
  - Insider alters IELTS exam score of an examinee for consideration;
  - Case registered under S.420, 467, 468, 471 and 120-B IPC r/w S.66 IT Act.
- Dr. Sudhir Kumar Goyal Vs. University of Delhi (2013): Delhi High Court:
  - Justice S.K.Mahajan Enquiry Committee, constituted by Governing Body, Satyawati College, to look into the irregularities, if any, in college administrations under Sports Quota;
  - Data Breach by using a USB Stick;
  - USB seized upon knowledge;
  - Petitioner files case of theft!
  - WP contesting departmental proceedings rejected;

Jailbreak!

- 2014: Pune: Court Clerk uses similar bail order; erases Petitioner names & types in names of Accused in murder case; forges signature of Court superintendent; prepares two fake bail bonds and forges court nazar's signature on them; Father of Accused befriended clerk;
- 2009: Ganga Singh Vs. State Of Haryana: Accused forge bail bonds of P & H High Court;

Sanctity of the Digital Signature

- 2015: T.P. Shivdas (CS) Vs. State Of Kerala (Ker High Court): Hospital management dispute; digital signature allegedly forged for uploading forms in the website of the Registrar of Companies. Bail granted;
- 2014: Sri Asish Bansal vs The State Of West Bengal (Cal. High Court): DS forged to appoint fake directors;
- 2014: J.Jayakrishnan Vs. ROC: detailed evidence to be led to decide forgery of Digital Signatures; ROC decision set aside;
- 2013: Shova Gurung Vs. State (P & H High Court): Digital Signatures of Company's Director forged and monies withdrawn;
- 2013: T.Vasudeva Pai Vs State (Kar. High Court): quashing refused though owner of Digital Signature purportedly gave letter denying forgery;

Takes the Cake

- DDPL Global Infrastructure Pvt. Ltd. Vs. Alok Mishra (2015) Bom High Court:
  - Digital Signatures forged to oust all 4 directors & to induct 2 new ones onto Company Board;
  - Accused allegedly used fake KYC to obtain digital signature in the name of one of the Directors;
  - Replaces the original DS on MCA website with this fake DS;
  - Alters constitution of the Board & tries to increase DDPL's share capital from Rs.5 cr to Rs.45 cr;

Insider – The Invisible Man (US, Aug 2015)

- 32 international traders & hackers involved;
- Global network of hackers (predominantly Ukrainian) hack into databases of Marketwired; P R Newswire Association; Business Wire and stole 150,000 unissued press releases pertaining to earnings, mergers and other corporate news of Caterpillar; Verisign; Edwards Lifesciences; Panera Bread and many more Companies;
- Traders sometimes provided hackers with "wish lists";
- US $100 million earned through such illegal trades using inside information;

Domain Names & Insiders

- 2015: Google Loses “google.com” for a minute!
- 2015: Topcon Positioning Systems, Inc. Vs. Jason W. Evans (WIPO Domain Name Dispute):
  - Former employee who managed Company’s domains holds them hostage;
- Demands over USD $800,000;
- Former employee directed to transfer password;

Are Courts Safe?

…. It Depends!

Courts Under Attack

- **June 22, 2016:** Anonymous launches DDOS attack on Minnesota Judicial Branch's website (www.mncourts.gov);
  - Emails the Star Tribune about attack;
  - Warns of more;
  - Website offline for a day;
- **Jan 13, 2016:** Anonymous attacks Thailand's Court website.
  - Reason? Death sentence to 2 Myanmar men for allegedly murdering 2 British tourists.
  - First attack? NO! Jan 5 – police sites attacked;
  - Only Court? No - 300 sites hacked!

Vigilantes & Justice

- Anonymous History:
  - **Nov 19, 2015:** Anonymous destroy ISIS Twitter accounts as counterblast to the Paris attack; US officials take 'secret pleasure';
  - Charlie Hebdo assault: Hacking collective's starting point against ISIS operation;
  - Helped track and share five ISIS-linked recruiters' details;
  - Disabled more than 5,500 Twitter accounts associated with ISIS;

Living in Denial

- Jan 24, 2014: U.S Federal Court Systems (www.uscourts.gov & other federal court websites) blocked by unidentified hackers;
- Denial of Service attack;
- Information on cases, electronic filing system i.e., Online filing of documents & online access for retrieval blocked;
- Offline for a day;

Hacks Galore

- 2016: Alpine Superior Court Website Hacked! (California Sub-Court):
  - "No Arab is superior over a non-Arab, and no white is superior over black nor a black over a white and superiority is by righteousness and God-fearing alone, Prophet Muhammad."
- 2015: Lagos State Government and the Court of Appeal websites hacked over Army-Shi'ite clash: Protest against maltreatment of Muslims in Nigeria;
- 2014: Barbados Supreme Court hacked: "Copres-DZ" claims responsibility. Sequel to "Royal Barbados Police Force" hack.
- 2014: Supreme Court of Canada, City of Ottawa & Ottawa police department websites down. Aerith's message: "This is just the start". "We will not rest, we have already hacked Ottawa police's mail server, stolen all email logs incoming and outgoing."

Love Thy Neighbors

- 2016: Gujarat High Court website hacked ("hcrec.guj.in")! Culprits? Alleged Pakistani Hackers;
  - Message: "PCA FAISAL 1337 Hacked by Faisal 1337 We are Team Pak Cyber Attackers";
- 2014: Lahore High Court Website hacked allegedly by Indian hackers;
  - Reason? Comments by Bilawal Bhutto on Kashmir & demanding retraction;
- 2011: Pakistan Supreme Court Website hacked: "Zombie_Ksa" asks for ban of pornographic sites and to help the poor;
  - Derogatory and abusive remarks about Court & Chief Justice;
- 2011: Bangladesh Supreme Court website hacked! Claims to be Bangladeshi Hackers allegedly stopping other hackers! – Pen test by hackers?

Rapid Fire

- 2012: Supreme Court of India & Congress websites

compromised: “#opindia”;

- “http://supremecourtofindia.nic.in, dot.gov.in & aicc.org.in” rendered inaccessible;
- Reason? Protesting against blocking of file-sharing websites like RapidShare & Vimeo.
- Message? “#Government must understand. #INTERNET belongs to us!

#TANGODOWN–> http://supremecourtofindia.nic.in & http://aicc.org.in”;

- “@Anon_Central Another #TANGODOWN –>> http://www.dot.gov.in Department of telecom, You should've expected us!”
- "We cannot let censorship happen... Operation India engaged,”

Data in the Legal World

- 2013: US: Washington State Court System attacked!

- 160,000 social security numbers, names, and driver's license numbers breached;

- More than a million Washington State residents exposed!

Implications?

- Courts not immune to cyber security threats;
- Inevitability of data breach or attacks
- Solution?
- **Identifying Court's data assets:** includes judges' orders, witness testimonies, pleadings, Roznama;
- **Identifying Threats:** Understanding and identifying risks; (Zero Day Vulnerabilities); Identifying attacks;
- **Process Driven Procedures:** From Causelists to Judgments;
- **Communications in the face of attacks:** Fall back to traditional modes!
- **Cyber security incident response team:** Resilience; backup; recovery;
- Backup Backup Backup;
- http://www.ncsc.org/~/media/Files/PDF/About%20Us/Committees/JTC/JTC%20Resource%20Bulletins/Responding%20to%20Cyber%20Attack%202-26-2016%20FINAL.ashx

THANK YOU

Q & A

N S NAPPINAI
ADVOCATE

nappinai@nappinai.com; nappinai@gmail.com;
+91-22 – 66330545; +91-22-66352604;