



Cyberlaws Consulting Centre  
World's 1st Integrated Cyberlaws Consulting Centre



**SETH ASSOCIATES**  
ADVOCATES AND LEGAL CONSULTANTS

# *Learning with Social Media*

## **Legal and Regulatory issues**

AUME 2010, 11December , 2010, Delhi  
Karnika Seth  
Cyberlaw Expert & Managing Partner,  
Seth Associates

All rights reserved copyrighted, 2010

# Introduction

- Seth Associates is a leading *full service Indian law firm* that is internationally networked to provide spectrum of legal services to its domestic and international clients
- We maintain one of the strongest Cyberlaws practice in India today.
- With more than a decade's experience in Cyberlaws Practice, Seth Associates recently established the World's first integrated '**Cyberlaws Consulting Centre**' at Seth Associates

# CCC- Cyberlaws Consulting Centre

- CCC renders cyber legal consultancy, cyber law analytics and forensic services to its clients world wide.
- Work experience of handling cybercrime matters with Delhi Police
- Delivered training workshops to Delhi police on dealing with cybercrime investigation cases
- *Recently authored a book titled '[Cyberlaws in the Information Technology age](#)' published by Lexis Nexis Butterworths that elucidates the key developments in the field of Cyberlaws across many important jurisdictions—India, United States and European nations*

# 'Cyberlaws in the Information Technology Age' by

www.lexisnexis.co.in

LexisNexis<sup>®</sup>  
Butterworths Wadhwa  
Nagpur

**Q:** Are you aware of key developments in the field of Cyberlaws across the important jurisdictions?



Cyber Laws in the  
Information Technology Age

Karnika Seth



LexisNexis<sup>®</sup>  
Butterworths Wadhwa  
Nagpur

ISBN: 978-81-8038-581-0 Price: 1495/-  
Year: 2009 Format: Hardcover

**A:** This book will introduce you to the subject...

### Salient Features

- ✦ Explains the fundamental concepts in cyberspace laws and aims to present a fair overview of the evolution of cyber laws across many jurisdictions.
- ✦ Discusses pertinent e-contracting and e-commerce issues, and describes popular e-payment systems and taxation regimes.
- ✦ Elucidates the key principles for determining jurisdiction in cyber law disputes, significance of electronic signatures and admissibility of e-evidence.
- ✦ An insight into other interesting cyberspace issues such as online privacy, defamation, freedom of speech on internet, intellectual property piracy on internet, and cybercrime issues with case studies and landmark precedents from different parts of the world.
- ✦ Provides practical tips on safeguarding one's security and privacy in the online world and will enlighten readers on their legal rights and obligations in cyberspace and legal implications of their actions on the Internet.
- ✦ Contains comparative assessment of cyber laws across different jurisdictions and critically comments on positive and negative traits of existing statutory framework, legal and policy frame work and important judicial precedents in information technology law and regulation.
- ✦ Appendices of existing cyber laws, international conventions, treaties and guide lines frame by International Organisations pertaining to cyber law and intellectual property, important EU Directives and cyber legislations of India, US, UK and other foreign countries are also given for easy reference.

**4**  
Easy ways  
to Buy\*

Customer Helpdesk Tel. +91-124- 4774477

Email: [orders.in@lexisnexis.com](mailto:orders.in@lexisnexis.com)

Visit us/Buy Online: [www.lexisnexis.co.in](http://www.lexisnexis.co.in)

Nearest Book Store

\* Always mention '0709ED25'

### LexisNexis

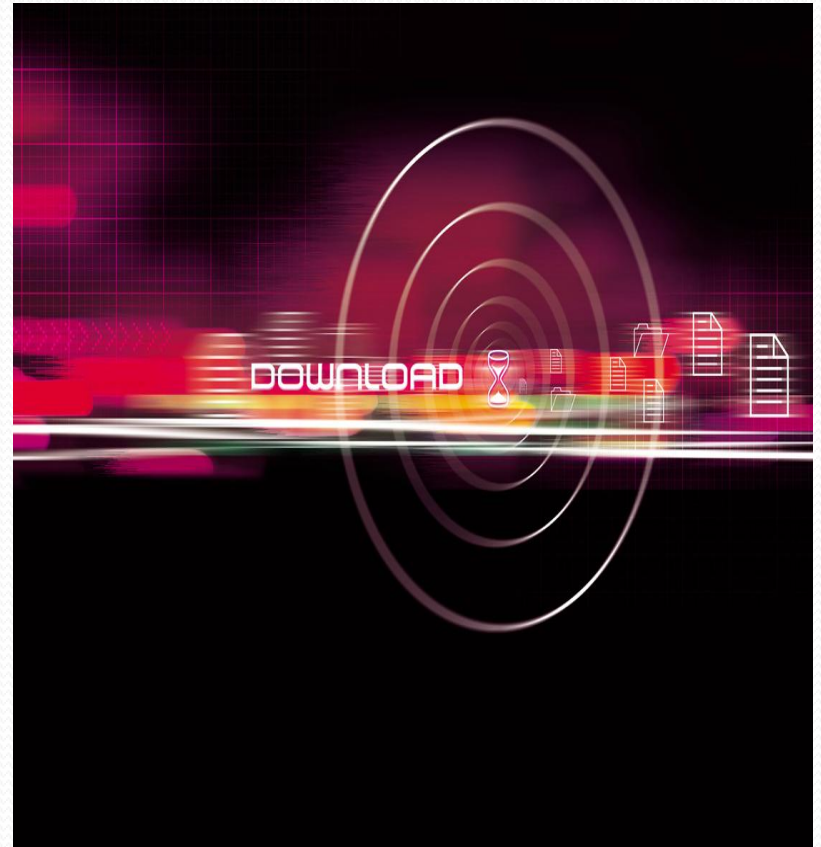
(A Division of Reed Elsevier India Pvt.Ltd.)  
14th floor, Tower B, Building No.10, DLF Cyber City,  
Phase II, Gurgaon – 122002, Haryana (India)  
Tel: +91 124 4774444 Fax: +91 124 4774100

Disclaimer: This is a promotional message from LexisNexis, a leading provider of authoritative legal, news, public records, and business information and electronic filing services. If you do not wish to receive commercial electronic email messages from LexisNexis, please send an e-mail with "unsubscribe" in the subject line to [unsubscribe.in@lexisnexis.com](mailto:unsubscribe.in@lexisnexis.com)

\*Terms and conditions apply. Offer is valid for a period of six months or till stocks are available.

# What is the Cyberspace?

- William Gibson in 1980s wrote a science fiction named *Neuromancer* wherein computer hackers waged war against secure data.
- *The setting had no physical existence and was named 'Cyberspace' by Gibson.*
- Unique features - dynamic, borderless space, anonymity, speed, cost effective, marked with rapid technological advances



# Regulating the Internet..

- Proponents of Cyberlaws believe that one's activities on the Internet need regulation by framing laws and rules that govern our activities in the cyberspace. This branch of law is termed as "Cyberlaws"
- **European Union, USA, UNCITRAL** framed important laws to govern cyberspace
- UNCITRAL Model law of e-commerce 1996
- EU data protection Directive
- DMCA Act 1998 in USA
- WIPO domain name dispute Resolution policy
- Critics who advocate 'no regulation' or 'self regulation' in the Virtual space believe that government should have minimum interference in regulating the cyberspace and its use of surveillance or censorship measures.
- **John Perry Barlow's** "Declaration of the Independence of the cyberspace" and **David G. Post,** *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521, 539 (1998)

# SOCIAL MEDIA LEARNING

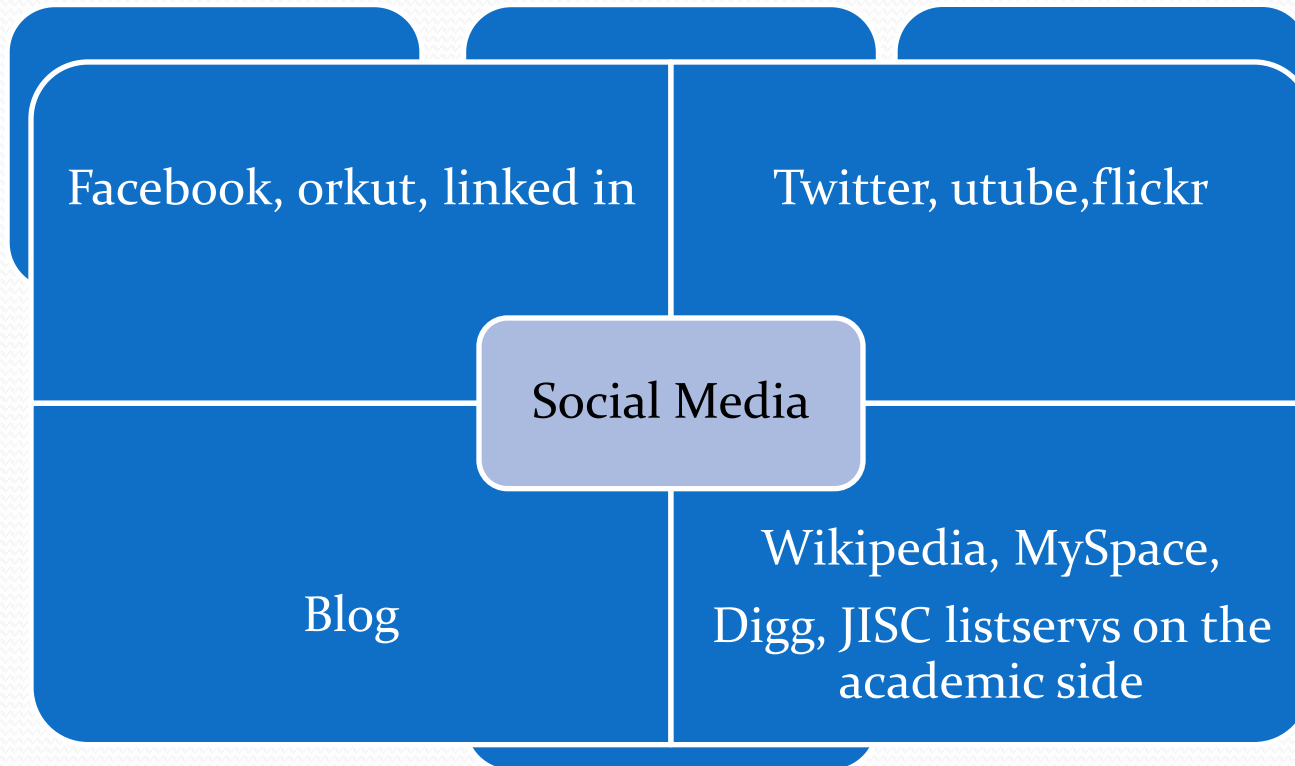
- Social networking and social learning are have created a global community in the cyberspace.
- Social media are online communications channels that utilize web technologies for social interactions by individuals in order to share, distribute, and disseminate information and knowledge.

# Social media learning community





# Few most powerful Social Media tools



# DO YOU KNOW?


- Facebook has more than 350 million active users.
- Facebook accounts for over seven percent of all web traffic.
- Mobile is even bigger than before for Facebook, with **more than 65m users accessing the site through mobile-based devices**. In six months, this is over 100% increase.
- Flickr now hosts more than **4 billion images**.
- Twitter recorded a growth of 1271 percent since 2008.

- Wikipedia currently has in excess of **14m articles**, meaning that it's 85,000 contributors have written nearly a million new posts in six months.
- LinkedIn has over 50m members worldwide.
- Nearly 500 Hospitals in U.S. use social media to interact with their patients, doctors and staff members.
- Eight in ten people believe that social media can enhance relationships with customers and clients.
- India is currently the fastest-growing country to use LinkedIn, with around 3m total users.

(Source: <http://trak.in/tags/business/2010/02/01/social-media-statistics-facebook-twitter-flickr-linkedin/> )

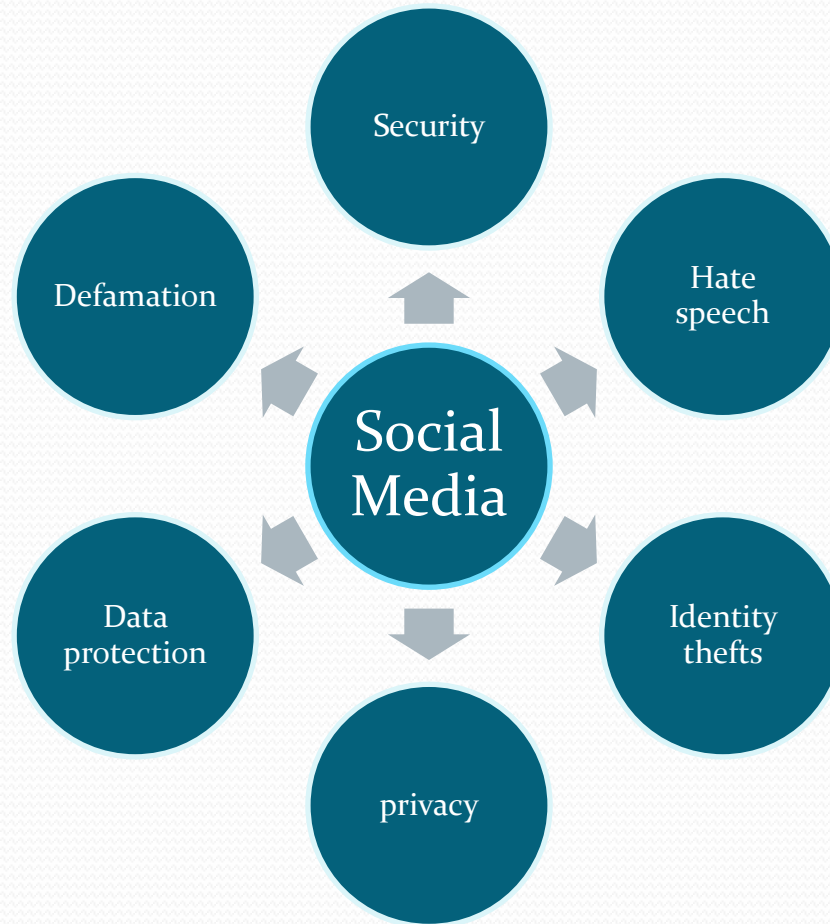
# Multiple benefits of Social Media learning

- 
- Build brand reputation
  - Improved customer relationships

- 
- Enhance employee morale
  - Enhance knowledge and awareness

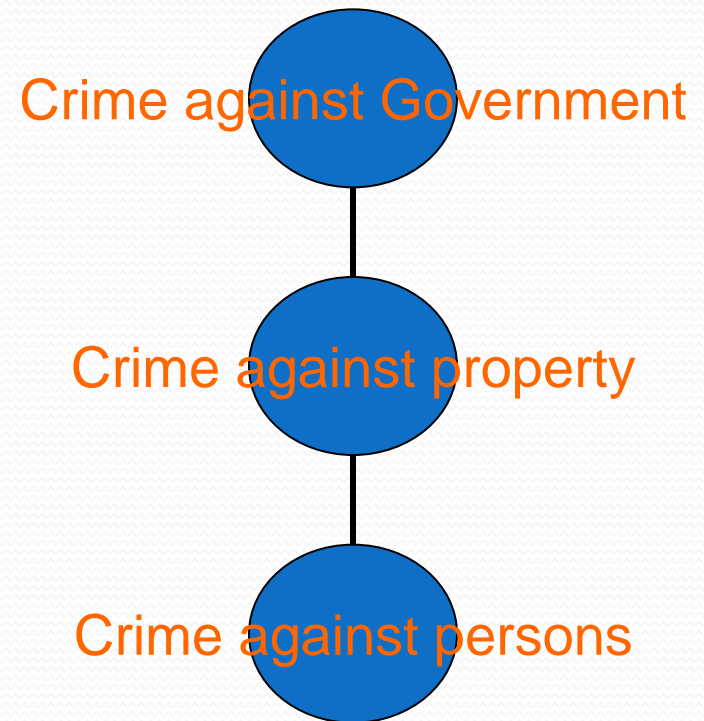
- 
- Best marketing tool
  - due diligence

# Legal challenges to Social Media learning



# Types of Cyber crimes

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phising
- Cyber terrorism



# The Information Technology Act, 2000

- The Information Technology Act 2000 came into force in India on 17 October 2000. It extends to whole of India and also applies to any offence or contraventions committed outside India by any person (s 1(2), IT Act 2000).
- According to s 75 of the Act, the Act applies to any offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

## Main Features of IT Act,2000

- Applicable to communications made through cell phones ,PDAs
- Conferred legal validity and recognition to electronic documents & digital signatures
- Legal recognition to e-contracts
- Set up Regulatory regime to supervise Certifying Authorities
- Laid down civil and criminal liabilities for contravention of provisions of IT Act,2000
- Created the office of Adjudicating Authority to adjudge contraventions



## Social Media learning -LEGAL ISSUES

- No homogeneous laws- UNCITRAL Model law on Electronic Commerce adopted by IT Act,2000
- **Data protection**- Section 43, 43A, 66,72 –Section 4,5 IT Act,2000
- Importance of secure electronic records and signatures-presumption in law for authenticity.
- **Right to privacy**- MMS, Cookies, bots
- Art. 21 of the Constitution –Section 66E, IT Act
- Employee surveillance issues- no policies on social media learning
- **Identity thefts**-Section 66C, cheating by personation – Section 66D,IT Act

## Glaring Examples – Data thefts



- *The incidents in the recent past involving Cyber Space have highlighted the issues of privacy and data protection in India*
- **The Pune scam** was the first among the many BPO frauds that made international headlines. In April 2005, five employees of **MsourceE in Pune** were arrested for allegedly pulling off a fraud worth nearly 2.5 crore rupees from the Citibank accounts of four New York-based account holders.
- In June 2005, the **British tabloid Sun**, in a sting operation, purchased the bank account details of 1,000 Britons from Karan Bahree, an employee of Gurgaon-based BPO company *Infinity E-Search*.

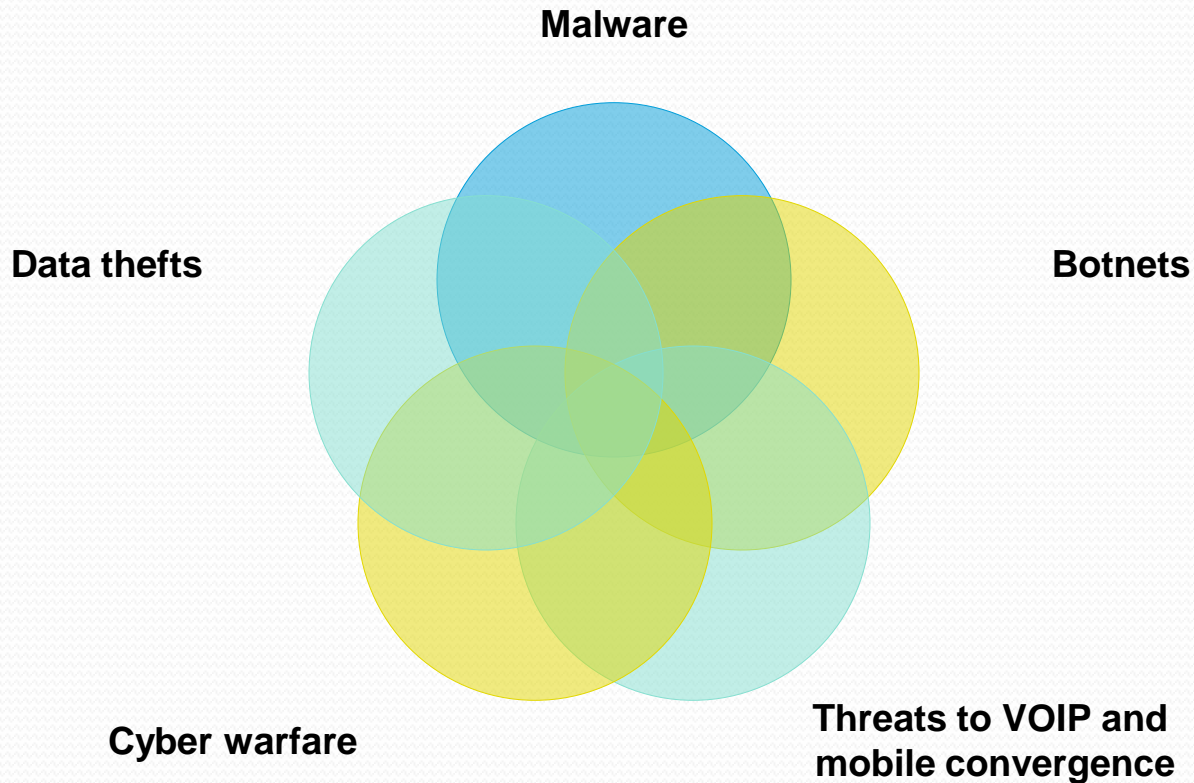
# The Noida MMS Scandal



- In February 2009, an MBA student in Noida a boy circulated video clip of his 23 -year-old-girlfriend doing striptease for him to his classmates using the girl's e-mail id.
- After the girl refused to marry him, the boy who had access to the girl's mail id and circulated that MMS clip to fellow students.
- Police registered a case of criminal intimidation following a complaint filed by the girl's family

# Cyber Threats in 2009 and Beyond

## Report of *Georgia Tech Information Security Center (GTISC)*





## Cybercrimes in 2009 and beyond...

<p>Malicious attackers will install malware on <b>social networking sites</b> leading to increased phishing scams, or stealing data,etc- browser level protection needed.</p>	<p>Hackers will install <b>malcode within video content</b> which will affect users accessing video clips.</p>
<p><b>Mash up technology</b> used by web applications to combine data/media from multiple sources, locations and coding styles may lead to increased corporate espionage and other scams</p>	<p><b>Identity thefts</b> will only increase and <b>botnets</b> will be used for corporate espionage and phishing scams</p>
<p><b>Polymorphic exploitation-</b> creation of unique exploit with each user request – signature based protection engines at network or host level fail</p>	<p>Growing popularity of VOIP applications- instances of <b>voice spam and voice phishing or smishing</b> will increase.</p>
<p><b>Targeted attacks</b> -Attack activity through e-mail, Instant messaging ,P2P networks will increase</p>	<p><b>Denial of service</b> affecting voice infrastructure</p>
<p><b>Cyber terrorist</b> attacks will increase and lead to cyber warfare- threat to nation's sovereignty</p>	<p><b>MMS scams</b> will be on the rise and raise issues of defamation and invasion of privacy</p>

## New cybercrimes post IT Amendment Act, 2009

Hacking – Section 66	Sending of offensive false messages(s.66 A)	Identity theft (s. 66C)
Cheating by personation (s.66D)	Violation of privacy (s.66E)	Cyber terrorism (s.66F)
Publishing sexually explicit content(s. 67A)	Child pornography (s.67B)	Stolen computer resource(s.66B)
Attempt to commit an offence (s.84C)	Abetment to commit an offence(s.84B)	

# Other Legal issues

- **Corporate espionage**
- **Intellectual Property Rights**- damages, injunction ,destruction of infringing materials.
- Ownership of content and control- most blogs disclaim liability for third party content
- Assume all rights granted by a user akin to an assignment of IP rights
- **Hate speech , freedom of speech** –Wikileaks
- **Online Defamation**- Section 499 and 500 IPC- 2 yr imprisonment . Section 66A of the IT Act,2000
- **Jurisdiction**- Section 1 and 75 IT Act,2000
- **Role and liability of intermediaries**- Section 79 IT Act,2000
- **Anonymity** , tracking the offender
- **Dispute Resolution and jurisdiction**- ODR, cybersettle, UDRP policy,etc

# OWNERSHIP OF CONTENT AND CONTROL

- While posting information on a social network the users generally believe that their profile, comments, photos and other information and their property under their exclusive control.
- But that's not really the case. They become often under the control of the web service provider or the intermediaries.
- Further the content posted by the user is guided by the content policies of the website which are generally very broad in nature and can put user at a difficult position.
- Comprise clickwrap agreements



# Case study

- **Linkedin** says “ non-exclusive, irrevocable, world-wide, perpetual, unlimited, assignable, sub licensable, fully paid up and royalty free right .....to copy, prepare derivative rights of, improve, distribute, publish, remove, retain, add, and use and commercialize in any way know known and in the future discovered....without any further consent, notice or compensation to you or to any third parties”.

# Cyber attacks...

YouTube - China-based network caught in cyber-espionage - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.youtube.com/watch?v=V8MzTNFJTcM

Most Visited Getting Started Latest Headlines

YouTube - China-based network ... us\_aers\_Deloitte Cyber Crime POV Jan...

**YouTube** cyber terrorism india video Search Browse Upload Create Account Sign In

## China-based network caught in cyber-espionage

Johannwyss82 109 Videos



0:12 / 1:54 360p

Johannwyss82 | March 30, 2009 | 1:54     **2,732**

A shadowy cyber-espionage network based mostly in China has infiltrated gover...

- How to Hack (BackTrack & VMware Player) 12,883 views J2897Tutorials 4:27
- Hacking the Power Grid 4,081 views MelihVision 3:22
- FBI Confidential -- China's Cyber Terrorism? 12,386 views ComingChinaWars 5:22
- Chinese cyber spies hack into government computers 1,358 views worldfocusonline 3:13
- The Canadian that Busted GhostNet 6,198 views TheHour 5:58
- Chinese, Russian cyberspies have penetrated the... 1,013 views cctvupload 3:21
- Forbes Discusses Chinese

Transferring data from tc.v12.cache6.c.youtube.com...

start National Seminar on ... Inbox - Microsoft Out... YouTube - China-bas... cyberlaw issue-opinio... 5:49 PM

# SECURITY



**Entrust IdentityGuard**  
Strong Authentication for your Enterprise

## Digital fingerprints to identify hackers

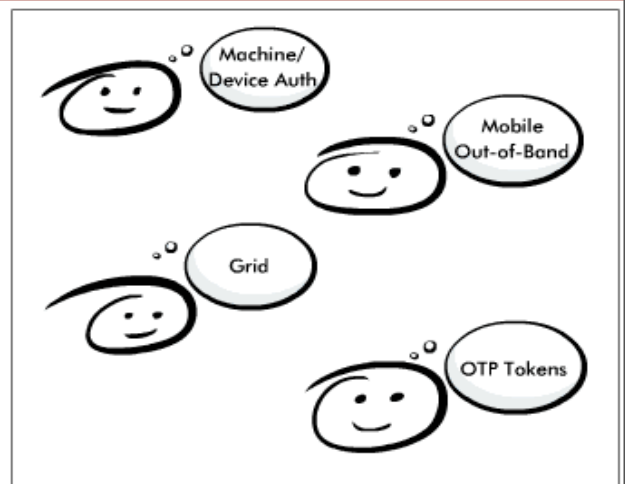
Posted on 27 January 2010.



How can you retaliate against a cyber attacker if you don't know who he is? As we have witnessed lately, attribution of an attack is quickly becoming one of the biggest problems that the US defense and cyber security community are facing at the moment.

According to Wired, DARPA, the agency of the US DoD responsible for the development of new technology for use by the military - and of the Internet - has accepted the challenge and will be starting Cyber Genome, a project aimed at developing a "cyber equivalent of fingerprints or DNA", so that the hacker can be conclusively identified. The project will be set in motion as early as this week.

The agency announced on Monday that they will strive to produce "revolutionary cyber defense and investigatory technologies for the collection, identification, characterization, and presentation of properties and relationships from collected digital artifacts of software, data, and/or users."



### LATEST NEWS » Friday, 02:37 EDT

- Twitter to establish information security program
- Man indicted for hacking and threatening the Vice President
- .org becomes first generic TLD protected by DNSSEC
- Wireshark in the large enterprise
- Phishing requires more effort than you might think
- IT pros expect network threats to increase as budgets decline
- How consumers influence data loss and breaches
- Rogue software details: Sysinternals Antivirus
- New book: Network Flow Analysis
- WhiteHat Sentinel: SaaS website vulnerability management
- Social networking "Bill of Rights" released
- Network Security Auditing

**wombat**  
security technologies

**Don't get caught by phishing attacks.**  
Protect yourself with Wombat Security Technologies' online security training and filtering solutions.

# Digital DNA to fight cybercrime

**"Digital DNA" to fight cyber crime | Homeland Security News Wire - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

http://homelandsecuritynewswire.com/digital-dna-fight-cyber-crime

Most Visited Getting Started Latest Headlines

**"Digital DNA" to fight cyber crime | ...**

## HSNW

HOMELAND SECURITY NEWSWIRE

Home Authentication / Biometrics Business / Finance Continuity / Recovery Cybersecurity Detection Education / Sci-Tech Emergency / Police / Mil.  
Government policy Infrastructure Public health / Biodefense Surveillance Systems Integration Transport / Border

THE BUSINESS OF HOMELAND SECURITY Friday, 25 June 2010 ADVERTISE SIGN UP FOR OUR FREE DAILY REPORT

Search

### "Digital DNA" to fight cyber crime

Published 6 November 2008

**Scottish researchers develop what they call "digital DNA": It is based on analyzing the way in which users access data on their computers and then creating a digital fingerprint that is unique to each user**

Computer experts at Edinburgh's **Napier University** have **secured** funding of £199,879 to help them pre-commercialize a digital fingerprinting and analysis software technique that could help companies crack down on computer fraud. The innovative patent-pending technology, called "digital DNA," is based on analyzing the way in which users access data on their computers and then creating a digital fingerprint that is unique to each user. Jamie Graves, a research fellow at Napier's School of Computing, explored the concept of digital DNA throughout his Ph.D.. Now, along with Professor Bill Buchanan, he has secured the two-year funding under the **Scottish Enterprise Proof of Concept program** to develop the software through to commercialization.

Graves believes that the digital DNA technique he has developed uses a particular metric that offers a far higher degree of proof probability that a certain person was behind any changes made to data. Criminal gangs are growing increasingly aware of the potential rewards of data theft. Court prosecutors, however, are seeking higher levels of proof when it comes to prosecuting data crime, particularly in areas such as auditing and compliance activity. "A weakness of the current system is that it is computer experts giving evidence on the basis that they believe a particular person accessed or changed data," said Graves. "What the digital DNA will do is give a much greater measure of

#### IN TODAY'S REPORT

- FAA brings flying car's day closer
- Bill seeks to bolster U.S. ability to fight bioterror
- George Mason University opens \$50 million biomedical lab to fight bioterrorism
- Administration moves ahead on Illinois prison purchase -- possible Gitmo replacement
- Lawmakers push for designating the Taliban a terrorist organization
- Pakistani court convicts, sentences 5 American for terrorism
- Marines to use autonomous vehicles built by Virginia Tech students

**CYBERSECURITY Sector Report**  
Read More

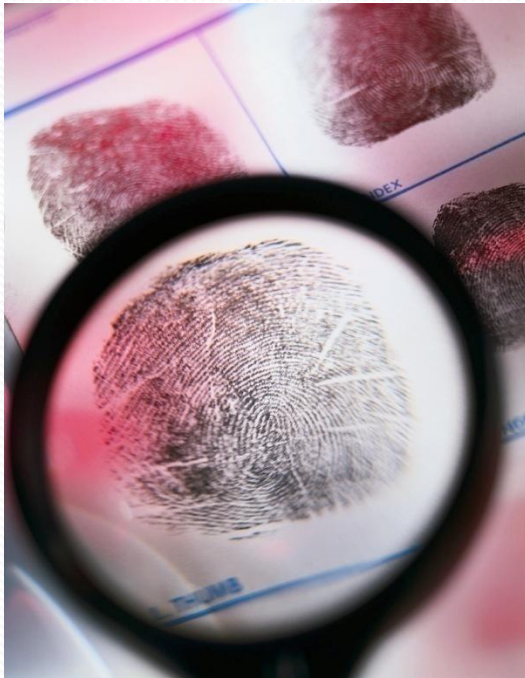
Done

start Inbox - Microsoft Out... "Digital DNA" to Fight ... 11:59 AM

## Caution : Internet Surveillance without technical or institutional restraint may infringe one's Right to Privacy

- *The new Internet filtering techniques allow for unlimited screening and are employed by governments without any technical or institutional restraint.*
- Most prominent has been the **OpenNet Initiative (ONI)**, a collaborative partnership between three leading academic institutions
- **'Magic Lantern' Trojan horse project**, initiated on occurrence of the 9/11 events in the USAFBI uses a 'light' monitoring tool called CIPAV
- In 2007, the German federal police came up with their own **'Bundestrojaner' (federal trojan)** project, but faced mitigation by the Federal Constitutional Court: the latter stated in February 2008 that trojanizing a suspect's computer was *'constitutionally permissible only if actual evidence of a concrete danger' existed, and that it was to be conducted only under judicial authorization (i.e. requiring a warrant)*

# Amendments- Indian Evidence Act 1872



- **Section 3** of the Evidence Act amended to take care of admissibility of ER as evidence along with the paper based records as part of the documents which can be produced before the court for inspection.
- **Section 4** of IT Act confers legal recognition to electronic records

## ***Societe Des products Nestle SA case***

**2006 (33 ) PTC 469**

- By virtue of provision of **Section 65A**, the contents of electronic records may be proved in evidence by parties in accordance with provision of **65B**.
- Held- Sub section (1) of section 65B makes admissible as a document, paper print out of electronic records stored in optical or magnetic media produced by a computer subject to fulfillment of conditions specified in subsection 2 of Section 65B .
  - a) The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by person having lawful control over the period, and relates to the period over which the computer was regularly used.
  - b) Information was fed in the computer in the ordinary course of the activities of the person having lawful control over the computer.
  - c) The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy.
  - d) Information reproduced is such as is fed into computer in the ordinary course of activity.
- ***State v Mohd Afzal,***  
**2003 (7) AD (Delhi)<sup>1</sup>**

# State v Navjot Sandhu (2005)11 SCC 600

- Held, while examining Section 65 B Evidence Act, it may be that certificate containing details of subsection 4 of Section 65 is not filed, but that does not mean that **secondary evidence** cannot be given.
- Section 63 & 65 of the Indian Evidence Act enables secondary evidence of contents of a document to be adduced if original is of such a nature as not to be easily movable.



# Presumptions in law- Section 85 B Indian Evidence Act

- The law also presumes that in any proceedings, involving **secure digital signature**, the court shall presume, unless the contrary is proved, that the **secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record**
- In any proceedings involving a **secure electronic record**, the court shall **presume, unless contrary is proved, that the secure electronic record has not been altered** since the specific point of time, to which the secure status relates

# Conclusions

- There are many legal and regulatory issues to be addressed vis a vis Social Media learning
- We need to devise social, technical and legal solutions to address these challenges
- Social e laws are evolving with time with social media learning curve
- Netizens and corporates are realising the importance of framing the Social Media policies
- Compliance with one's jurisdictional statutory laws is mandatory
- One also needs to adopt best practices of netiquette and ensure security parameters on cyberspace
- In the end, most importantly, due caution ought to be adopted by netizens to preserve one's identity in cyberspace –Section 42 IT Act,2000-control of private key.

# Thank you!



Cyberlaws Consulting Centre  
World's 1st Integrated Cyberlaws Consulting Centre

## **SETH ASSOCIATES**

ADVOCATES AND LEGAL CONSULTANTS

***New Delhi Law Office:***

C-1/16, Daryaganj, New Delhi-110002, India

Tel: +91 (11) 65352272, +91 9868119137

***Corporate Law Office:***

B-10, Sector 40, NOIDA-201301, N.C.R, India

Tel: +91 (120) 4352846, +91 9810155766

Fax: +91 (120) 4331304

E-mail: [mail@sethassociates.com](mailto:mail@sethassociates.com)