*International Journal of Information Technology and Management*

*Vol. VII, Issue No. X, November-2014, ISSN 2249-4510*

# THE SURVEY STUDY ON MAINTAINING OF DATA PRIVACY AND SECURITY THROUGH CYBER LAW

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VII, Issue No. X, November-2014, ISSN 2249-4510

# The Survey Study on Maintaining Of Data Privacy and Security through Cyber Law

**Pelasur Chandrakumar Swamy**

Research Scholar, Himalayan University, Arunachal Pradesh

***Abstract – Computer crime issues have become high-profile, particularly those surrounding hacking, copyright infringement through warez, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extraterritorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.***

***Keywords: Jurisdiction, Particularly, Privacy, Lawfully, Information, Hacking, Limitations, Data Privacy, Security, etc.***

----------♦----------

## INTRODUCTION

Another major problem of cyber law lies in whether to treat the Internet as if it were physical space (and thus subject to a given jurisdiction's laws) or to act as if the Internet is a world unto itself (and therefore free of such restraints). Those who favor the latter view often feel that government should leave the Internet community to self-regulate. The governments of the world and stated, "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different". A more balanced alternative is the Declaration of Cyber secession: "Human beings possess a mind, which they are absolutely free to inhabit with no legal constraints. Human civilization is developing its own (collective) mind. All we want is to be free to inhabit it with no legal constraints. Since you make sure we cannot harm you, you have no ethical right to intrude our lives. So stop intruding!" Other scholars argue for more of a compromise between the two notions, such as Lawrence Lessig's argument that "The problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once" Computer crime encompasses a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories:

(1) Crimes that target computer networks or devices directly

(2) Crimes facilitated by computer networks or devices.

## REVIEW OF LITERATURE:

A common example is when a person starts to steal information from sites, or cause damage to, a computer or computer network. This can be entirely virtual in that the information only exists in digital form, and the damage, while real, has no physical consequence other than the machine ceases to function. In some legal systems, intangible property cannot be stolen and the damage must be visible, e.g. as resulting from a blow from a hammer. Where human-centric terminology is used for crimes relying on natural language skills and innate gullibility, definitions have to be modified to ensure that fraudulent behavior remains criminal no matter how it is committed. A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators. Specific computer crimes are:

- Spam

- Fraud
- Obscene or offensive content
- Harassment
- Drug trafficking
- Cyber terrorism etc.

**1- Contemporary cybercrime:**

In addition to its socio-economic benefits, there is no doubt that computer technology and the internet – just as with other means enhancing capabilities of human interaction – can be used for criminal activity. While computer-related crime, or computer crime, is a comparatively long-established phenomenon, the growth of global connectivity is inherent to contemporary cybercrime. Computer-related acts including physical damage to computer systems and stored data; unauthorized use of computer systems and the manipulation of electronic data; computer-related fraud and software piracy have been recognized as criminal the United Nations Manual on the Prevention and Control of Computer Related Crime noted that fraud by computer manipulation; computer forgery; damage to or modifications of computer data or programs; unauthorized access to computer systems and service; and unauthorized reproduction of legally protected computer programs were common types of computer crime. These acts may include all of the computer-related crimes listed above, in addition to many others, such as those related to computer or internet content, or computer-related acts for personal or financial gain. As set out in this Chapter, this Study does not 'define' contemporary cybercrime as such. It rather describes it as a list of acts which constitute cybercrime.

**2- Cybercrime as a growing challenge:**

The increasing ubiquity of global connectivity presents a serious risk that rates of cybercrime will increase. While reliable statistics are hard to obtain, many country respondents to the Study questionnaire indicated that cybercrime is a growing challenge – a plausible viewpoint given underlying criminological and socio-economic factors. Due to significant challenges in the measurement of cybercrime, cross-nationally comparative statistics on cybercrime are much rarer than for other crime types. Annex Two to this Study examines current methodological approaches to measuring cybercrime, and presents some of the few available statistics In the past five years in particular, the issue of cybercrime has come prominently to the forefront of public discussion, including in developing countries. A search of global news wires for the terms 'cybercrime' and 'homicide', in the six official United Nations languages, reveals a significant relative growth in the frequency of global news references to cybercrime, as compared with references to homicide. Between the years 2005 and 2012, references to cybercrime have increased by up to 600 per cent, compared with around 80 per cent in the case of references to homicide. Such measurements are not directly related to underlying cybercrime acts. Nonetheless, they can reflect general global 'activity' concerning cybercrime – including media reporting on government initiatives and counter measures.

Cybercrime has also taken on a global scale, with criminals basing themselves in countries with little or no legislation against cybercrime. However, with international instruments such as the Council of Europe's Convention on Cybercrime 2001, ratification of such a treaty by countries could prove extremely valuable in fighting cybercrime at an international level. Although many countries have signed, only a few have ratified it, and the legislative and enforcement authorities in many countries are slow on the uptake. Countries should be aware, however, that, with the current pace of technological developments, the international dimension of cybercrime, and consequently of cybersecurity, is yet unchartered. The targets of attacks affect the whole of the internet and although, at the moment, the main targets are private companies and individual end users, it will not be long before attacks on critical infrastructure become common.

**CONCLUSION:**

The survey will suggest that the creation of a model law would reduce the cost and challenges for legal systems that have not yet addressed spam issues, stating that these countries could enact and implement the law, with confidence that it approaches a set of best practices in this area. The analysis, however, underlines that a model law is not an instant solution to the spam problem. Cleaning up spam is a question of resources, enforcement and the effective integration of anti-spam laws with existing technology, market and norms-based approaches. Regulators will have to work closely with technical experts to track spammers down and collect electronic evidence of laws, but also of effective enforcement. This problem has become increasingly important over the past few years, as a significant percentage of spam promotes some type of fraud against the recipient, from phishing scams to viruses used for denial of service attacks, including illegal financial schemes and offers for products of dubious quality or legality. One feature of international and regional cybercrime instruments, the inclusion of specialized investigative powers not usually found in non-cyber specific instruments. As the world moves towards universal internet access, it may be that conceptions of cybercrime will need to operate on a number of levels: specific and detailed in the case of the definition of certain individual cybercrime acts, but sufficiently broad to ensure that investigative powers and international cooperation mechanisms can be applied, with effective

safeguards, to the continued migration of offline crime to online variants.

## REFERENCES:

1. The UCLA Online Institute for Cyberspace Law and Policy. *A&M Records v Napster: MP3 File Sharing Disputes Continue in the Aftermath of Recent Court Rulings*, www.gseis.ucla.edu/iclp/napster.htm

2. Critique of the Proposed UK Implementation of the EU Copyright Directive, by Julian T. J. Midgley (jtjm@ukcdr.org), Campaign for Digital Rights: www.ukcdr.org/issues/eucd/ukimpl/

3. National Institute of Standards and Technology, *Computer Security: Recommendation for Key Management – Part 1: General (Glossary of Terms and Acronyms)*, by Elaine Barker, William Barker, William Burr, William Polk and Miles Smid. NIST Special publication 800-57, April 2005.

4. Explanatory Notes to Electronic Communications Act 2000, Chapter 7, http://www.opsi.gov.uk/acts/en2000/2000en07.htm

5. Digital Music Usage and DRM: Results from a European Consumer Survey by Nicole Dufft, Andreas Stiehler, Danny Vogeley, Thorsten Wichmann, May 24, 2005.

6. Electronic Frontier Foundation: Unintended Consequences: Five Years under the DMCA, September 24, 2003. www.eff.org/

7. African Union, 2012. Draft Convention on the Establishment of a Legal Framework Conductive to Cyber security in Africa (Draft African Union Convention).

8. Common Market for Eastern and Southern Africa (COMESA), 2011. Cybersecurity Draft Model Bill. (COMESA Draft Model Bill).

9. The Commonwealth, 2002. (i) Computer and Computer Related Crimes Bill and (ii) Model Law on Electronic Evidence (Commonwealth Model Law).

10. Commonwealth of Independent States, 2001. Agreement on Cooperation in Combating Offences related to Computer Information (Commonwealth of Independent States Agreement).

11. Council of Europe, 2001. Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Council of Europe Cybercrime Convention/Protocol).

12. Economic Community of West African States (ECOWAS), 2009. Draft Directive on Fighting Cybercrime within ECOWAS (ECOWAS Draft Directive).

13. European Union, 2000. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (EU Directive on e-Commerce).

14. Shanghai Cooperation Organization, 2010. Agreement on Cooperation in the Field of International Information Security (Shanghai Cooperation Organization Agreement).

15. United Nations, 2000. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (United Nations OP-CRC-SC).