

THOUGHTLEADERS

PRASHANT MALI | prashant.mali@cyberlawconsulting.com



ADVOCATE PRASHANT MALI is the President - Cyber Law Consulting.

Challenges with Cloud Computing

While cloud offers many benefits, it also brings in legal complexities.

WITH cybercrime having grown out of infancy, gaining professionalism and proving to be a bold threat to individuals, businesses and institutions of all kinds alike, paradigm shifts in the way we use information technology come as a mixed blessing: cybercriminals do not only gain profit from the same benefits available to regular customers, but are also among the first to detect and exploit loopholes and other side effects of new technologies. In cloud computing, such a paradigm shift is taking place right now.

The increasing use and opportunities of cloud computing services hold many challenges for legal practitioners, especially with respect to data protection policies. However, the effects of cloud computing on the law enforcement community can be narrowed down to one essential aspect of criminal investigations: the acquisition of evidence. While there are some beneficial developments, the loss of location is likely to cripple cybercrime investigations at a very early stage.

The loss of location

Data in the clouds is constantly shifted from one server to the next, moving within or across different countries at any time. Also, data in the

clouds might be mirrored for security and availability reasons, and therefore could be found in multiple locations within a country or in several separate countries. Due to this and to cached versions of data, not even the cloud computing provider might know where the sought-after data is exactly located. Thus, one could say that location as a constant applicable to all tangible objects and having been applied to intangible data objects ever since the Internet became popular as well, has ceased to function under the conditions of cloud computing.

Location, however, is of prime importance to deduct the applicable jurisdiction in order for law enforcement authorities to gain access to a certain object other than publicly accessible information, such as text on a web page, especially if coercive powers are needed to retrieve the object. This comes as a consequence to the international legal principle of territorial sovereignty which sets forth that no state may enforce its jurisdiction within the territory of another sovereign state.

Since the location of data often cannot be determined at a given time nor predicted for a given time in the future by law enforcement authorities, the determination of jurisdiction

concerning data in the clouds would be based on coincidence; and utilising the help of cloud computing providers before determining data location could lead to forum shopping. Both outcomes hardly fit the needs of the rule of law in criminal proceedings. In finding viable solutions for investigations in the clouds, it might therefore prove fruitful to think beyond the principle of territoriality.

Benefits for investigation

In spite of the confusion concerning location and jurisdiction outlined above, the rise of cloud computing also creates beneficial effects for law enforcement authorities that should not be left unconsidered: Since cloud computing applications allow for a greater flexibility in workflows of all kinds, many individuals as well as cybercriminals embrace the opportunities that services like Google Mail and Google Docs, Dropbox or Evernote are offering. Hence, information that without cloud computing services might have been stored on easy to conceal media such as tiny memory cards or flash drives in all kinds of unsuspecting hardware such as navigation devices:

"The increasing use and opportunities of cloud computing services hold many challenges for legal practitioners."



--required physical access to obtain for future use as evidence;

--never been created in the first place is likely to be created, stored and found within the clouds and thus easily accessible at a technical level.

Provisions for the extended search and seizure of computer data on connected systems such as Section(80) on The Information Technology Act,2000 as amended by The Information Technology(Amendment) Act,2008 may enter any public place and search and arrest without warrant any person who is reasonably suspected of having committed or of committing or of being about to commit any offence under the above said Act.

How to deal with the loss of location

So far it has been shown that location is not a factor to which legal strings can be attached when dealing with data in the clouds. Simply not being able to access vital evidence due to uncertainty about the applicable jurisdiction is not an option, however, since the states' mandate and obligation to prosecute crimes in cyberspace is of the utmost importance not only to victims, but also to stakeholders at a private and institutional level within national as well as international contexts. Therefore, different approaches need to be evaluated. Have a closer look at existing options as well as models in comparable legal fields and try to develop a different approach beyond the principle of territoriality.

Access using CrPC Sections

As already mentioned, the information in a network environment need not be stored at the same site. The data could reside at a remote location even in a different country.

Therefore, it may be important to find out the storage location and take action accordingly. In case, storage of data is suspected to be located outside the country, it may be necessary to alert the Interpol and take necessary follow up steps to issue letters rogatory under the provisions of Section 166 A CrPC.

Additional conditions and safeguards

As much as the power of disposal approach brings feasibility for law enforcement authorities, it is suited to infringe upon the rights of suspects and/or third parties: it might, for example, not seem appropriate to enable law enforcement authorities to look into an Evernote or Dropbox account and thus to read intimate thoughts of someone who has been pressed charges against due to an alleged defamation or political speech. Also, data stored in the cloud usually can be classified as content data; the contents of telecommunicative actions, however, receive special fundamental protection in many countries. Logging on to a Google Mail account, for example, would infringe the right to privacy provided by Article 21 of The Constitution of India and also right to telecommunication secrecy provided in Germany by Article 10 paragraph 1 of the German Constitution. If done in a covert manner instead of openly, such an infringement usually requires a court order or permission from Home Secretary beforehand.

Government of India can invoke Section 69 of The IT Act,2000 for interception or monitoring or decryption of any information through any computer resource. This section is violative of Article 21 of Indian constitution as mentioned above.

In order to alleviate the possible effects on fundamental rights, additional conditions and safeguards should be considered. Such conditions and safeguards could be

- limiting the scope of application to cases with yet to be defined exigent circumstances, including those where it is believed evidence will be destroyed if not seized;

- stipulating the requirement for a judicial order;

- stipulating notification obligations, both notifying the account holder and the provider, possibly with restrictions for cases in which the outcome of an investigation might be endangered;

- stipulating obligations to mark the



Government of India can invoke Section 69 of The IT Act,2000 for interception or monitoring or decryption of any information through any computer resource.

data that has been obtained, accompanied by scheduled deletion obligations.

Conclusion

The rise of cloud computing provides cybercriminals as well as law enforcement authorities with new opportunities. The downturn for the law enforcement community, however, comes with the loss of location caused by cloud computing technology. Since the principle of territoriality requires location as a prime legal connecting factor for investigatory measures in criminal procedure, a new legal instrument is to be found in order to prosecute cybercriminals and obtain digital evidence in the clouds. Furthermore, traditional concepts of jurisdiction usually resort to criteria which are not applicable to the digital world. Therefore, a new legal instrument would have to regard location as irrelevant and serve as manageable parameter with respect to both the legal world and the world of information technology. Such a regulation might be built upon the legal connecting factor of (formal) power of disposal. [\[6\]](#)