Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 31 August 2010

Discussion paper

Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?

Project funded by Romania, Estonia, Monaco, Microsoft, McAfee and the Council of Europe

This discussion paper has been prepared by Jan Spoenle (Germany) for the Economic Crime Division of the Council of Europe (Directorate General of Human Rights and Legal Affairs) within the framework of the global Project on Cybercrime.

Contact

For comments or further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Contents

1 Introduction: about cloud computing

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.

Before the 1980s, computing was done by large mainframe computers, where a single machine served many users. After that, the client-server model allowed for a distribution of computational tasks within a network, though the usually smaller office client machine still requires to run software of its own, which has to be configured and administered by the client user. In cloud computing, however, almost all computational tasks including the installation, configuration and administration of adequate software are taking place within the cloud – a multitude of servers connected among each other and accessible via the Internet, often through a web interface, thus forming a "cloud" of computational power. In contrast to the mainframe age, many machines now serve single users.

There are different flavours of cloud computing like IaaS and Saas;[1] however, since the underlying principle is the same, the differences do not matter in terms of effects on criminal investigations. What matters to prosecutors and investigators are the use cases not only available to sophisticated and organized cybercriminal gangs, but also to regular Internet users, as more and more people shift parts of their lives into digital realms, which already leads to rising numbers of crimes against the confidentiality, integrity and availability of computer data and systems (so-called CIA offences[2]). Therefore, in order to understand the problems posed by cloud computing, it might prove useful to pick two wildly popular use cases of this technology and explain their ramifications – Google Mail and Dropbox.[3]

Google Mail provides e-mail services in a variety of ways: it's a webmail service, so users can access it via their Internet browser of choice without the need to install and use an e-mail client. Using the latter, however, is also possible, enabling users to receive their e-mail over POP or IMAP protocols. And last but not least, there are dedicated clients for certain mobile equipment such as Android OS smartphones[4] offering always-on modes where e-mail will be delivered instantly. Common to all these services is the underlying principle of cloud storage: every e-mail sent and received through Google Mail as well as every attached file will be stored by Google Inc. within its "cloud" of servers scattered all over the world; Google provides several gigabytes of storage for each individual user. Due to positive effects in terms of availability, power consumption and costs, the users' data is constantly moved around within the "cloud" by algorithms. Therefore, it's always possible to access a certain e-

[1] These acronyms translate to „Infrastructure as a Service" and „Software as a Service"; for details see *Schwerha IV, Joseph J.*, „Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from „Cloud Computing Providers", Project on Cybercrime discussion paper, January 2010, available electronically in PDF format from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf and *Spies, Axel*, „Cloud Computing – Schwarze Löcher im Datenschutzrecht", Multimedia und Recht issue 5 (2009), pp. XI – XII.
[2] See Articles 2 – 6 of the Budapest Convention on Cybercrime.
[3] See http://mail.google.com and http://www.dropbox.com.
[4] See http://www.android.com.

mail message; however it's not possible to tell where exactly the data representing this certain message might be located.

Dropbox Inc. offers storage services for all kinds of files. Other than Google Mail, Dropbox limits free storage to 2 gigabyte, but users can pay for a premium account and, depending on their monthly budget, use as much as 100 gigabytes to store files within their online folders. Dropbox, as well as many competitors offering similar online storage solutions, allows sharing of files with other people, either protected by a password or openly accessible, for other Dropbox users as well as for general Internet users without the need to have a Dropbox account themselves. Therefore, it's an ideal solution for many needs, being one of them to outsource the storage of important files a perpetrator does not want to be discovered in a police raid. Like Google, Dropbox uses servers in different countries to store their users' data, which is being moved around constantly to minimize costs and maximize availability. Once again, the files stored in Dropbox folders are accessible at any time, but their exact location at a certain point of time is practically indeterminable.

2 Effects on criminal investigations

The increasing use and opportunities of cloud computing services hold many challenges for legal practitioners, especially with respect to data protection policies.[5] 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.

2.1 The loss of location

As explained above, 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.[6] 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.[7]

If cloud computing were only to cause serious delays and complicate the process of determining the sovereign state to which law enforcement authorities would have to turn to for mutual assistance and cooperation concerning an ongoing investigation, the

[5] See for example *Weichert, Thilo*, „Cloud Computing und Datenschutz", available online from https://www.datenschutzzentrum.de/cloud-computing/; *Spies, Axel*, „Cloud Computing – Schwarze Löcher im Datenschutzrecht", Multimedia & Recht (MMR) issue 5 (2009), pp. XI – XII.
[6] See *Schwerha IV, Joseph J.*, Project on Cybercrime discussion paper, January 2010, loc. cit., pp. 9 – 10; *Nägele, Thomas/Jacobs, Sven*, „Rechtsfragen des Cloud Computing", Zeitschrift für Urheber- und Medienrecht (ZUM, 2010), pp. 281 – 292 (289).
[7] Generally on the principle of territoriality *Stein/von Buttlar*, Völkerrecht, Cologne, 11th ed. 2005, pp. 186 – 196; *Ipsen, Knut*, Völkerrecht, Munich, 5th ed. 2004, pp. 310 – 318.

principle of territoriality could be obeyed nonetheless. However, 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 utilizing 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.[8]

2.2 Benefits

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[9] 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 unsuspicious hardware such as navigation devices;
- 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 Article 19 paragraph 2 of the Budapest Convention on Cybercrime of the Council of Europe[10] already grant access to files that can be accessed and obtained lawfully from a computer which itself must be subject to a lawful search:

> Article 19 – Search and seizure of stored computer data
>
> 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

However, Article 19 paragraph 2 of the Convention refers to computer systems or parts of it that are located within the territory of the respective authority's state only.

A good example for such beneficial effects can be found in a FBI spam case against Pulse Marketing, where agents were able to obtain incriminating spreadsheets the

[8] This issue has been brought up by scholars past and present, see e.g. *Sussmann, Michael A.*, „The Critical Challenges From High-Tech And Computer-Related Crime At The Millenium", 9 Duke Journal of Comp. & Int'l L. 451, 454 – 455 and 470 – 473 (1999); *Schwerha IV, Joseph J.*, Project on Cybercrime discussion paper, January 2010, loc. cit., pp. 18 – 19. See also below section 3.

[9] Evernote is a cloud-based and highly sophisticated notebook, accessible via the web, client software and multible portable devices such as iPhone or Android smartphones, see http://www.evernote.com.

[10] This clause has already been implemented in some countries, e.g. in Germany in Section 110 subsection 3 of the German Criminal Procedure Code (Strafprozessordnung, StPO).

perpetrators worked on in a collaborative way through Google Docs.[11] Although, in this case, it obviously was possible to apply U.S. federal jurisdiction by the local authorities, clearly the development of a general principle on access to data of unknown location within the Budapest Convention framework would better serve the needs of law enforcement authorities worldwide and Internet users alike.

3 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. This report will 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.

3.1 Existing solutions

3.1.1 Access with consent – Article 32 lit. b CCC

The Budapest Convention on Cybercrime already features a legal principle which overrules location as a legal connecting factor: Consent. Article 32 of the Budapest Convention states:

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
>
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

After implementing the Convention on Cybercrime, a country's authorities are enabled to look into and secure data for later use as evidence as long as they act with consent of the person who has the lawful authority for such disclosure, even if the data is not located within the authority's territory. The person with lawful authority to disclose the sought data does not necessarily have to be the suspect or another individual person; it can also be a legal entity – the cloud computing provider, for example.[12] It is understood that the requested person is physically on the territory of the investigating authority when consenting.

However, regarding the utilization of Article 32 lit. b of the Convention within the cloud computing scenario, there are two major flaws: First, even if the consent does not have to be obtained from the least likely person to voluntarily agree – the suspect –, the cloud computing provider might side with its clients, ranking data protection and privacy higher than criminal investigations, thus making coercive powers and time-

[11] See *Poulsen, Kevin*, Wired Magazine: http://www.wired.com/threatlevel/2010/04/cloud-warrant/ (last accessed in August 2010).
[12] See *Schwerha IV, Joseph J.*, Project on Cybercrime discussion paper, January 2010, loc. cit., p. 18.

consuming mutual legal assistance necessary; the cloud computing provider also might not even have the lawful authority to disclose, depending on applicable data protection provisions. Second and more obvious, the data might to a certain extent of probability not be located within the territory of any Party to the Convention.

In fact, if it is not possible to determine the location of the data sought, using Article 32 lit. b of the Budapest Convention in an investigation might even be considered a procedural error. Therefore, consent as a legal connecting factor currently does not make up for the loss of location; Article 32 lit. b of the Budapest Convention can only be applied if the data location is known.

3.1.2 Exceptions from the principle of territoriality

International criminal law does not only know the principle of territoriality – which is the main legitimate connecting factor for the exercise of sovereign power –, but also exceptions from it such as the effects principle, the flag principle and the principle of nationality.[13] Since the territoriality principle is the main obstacle for investigating actions within the clouds, given exceptions might prove helpful in finding an approach to obtain critical data from cloud computing providers. However, most of these exceptions are tailored to serve the needs of substantive criminal jurisdiction, i.e. to determine a state's right to and responsibility for a criminal prosecution, subsequent trials and punishment. With respect to cloud computing as a challenge to the prosecution of cybercrime, the authorities of the prosecuting state usually already have assumed jurisdiction. Therefore, the question to be targeted isn't whether or not a crime can be prosecuted within a certain country at all, but whether or not certain procedural actions can be taken regardless of location. Thus, the effects principle as well as other factors used to prioritize conflicting jurisdictional claims[14] can be safely ruled out as model legal connecting factors for data in the clouds, leaving the flag principle and the principle of nationality as possible templates for a new approach to determine access to such information.

3.1.2.1 Flag principle

The flag principle basically states that crimes committed on ships, aircraft and spacecraft are subject to the jurisdiction of the flag state, regardless of their location at the time of the crime.[15] It is also reflected in the Budapest Convention on Cybercrime.[16] Although it ties jurisdiction to a physical source – the respective ship or craft – the flag principle allows for procedural actions taken regardless of location since the moveable flagged object is perceived as an extension to the territory of the flag state.

In order to possibly make this idea fruitful for the cloud computing scenario, one has to bear in mind that the clouds might not be the actual place where a crime has been committed. Another conceptual difference is the absence of a physical source, as the location of the physical storage media is unknown and the sought-after data itself is not a physical object. However, there is also some commonality: Like an aircraft in flight, a ship on the high seas or a spacecraft in transit, data in the clouds is constantly moving. And via the use of metadata, the origin of data might be deducible in some cases, thus establishing a "flag state" to tie the data to – this is the case with geo-

[13] See *Ambos, Kai*, Internationales Strafrecht, Munich, 2nd ed., 2008, pp. 24 – 26.
[14] See e.g. *Brenner, Susan W.*, „Cybercrime Jurisdiction", Crime Law Soc Change, issue 46 (2006), pp. 189 – 206 (198 – 206).
[15] See *Ambos, Kai*, Internationales Strafrecht, Munich, 2nd ed., 2008, pp. 32 – 36 for more on the flag principle.
[16] See Article 22 Paragraph 1 lit. b, c of the Convention.

tagged pictures, for example, and documents might be geographically allocated by metadata hinting towards localized software used for their creation.

Unfortunately, however, this information will not be revealed unless an investigator is actually allowed to look into the data – unlike flags on ships etc., which can be easily spotted and identified. Therefore an approach that would grant the "flag state" of sought-after data access to information stored in the clouds for means of criminal investigations would be flawed from the beginning. Also, in the not unlikely event of a failure to allocate data to any country, a flag principle approach would be of no use; the same is true for cybercrime investigations involving information that might have been created in more than one country by mobile or foreign perpetrators. To sum things up, the flag principle does not provide a viable solution to circumvent the principle of territoriality for access to data in the clouds.

3.1.2.2 Principle of nationality

Another way to circumvent territorial issues can be found within the principle of nationality. It uses the nationality of the perpetrator as legal connecting factor to establish criminal jurisdiction[17] and is based on the principle of "aut dedere, aut iudicare", which is also reflected in the Budapest Convention on Cybercrime.[18]

Using nationality as legal connecting factor to establish access to data in the clouds, however, faces some serious concerns: On the one hand, perpetrators in a cybercrime case might easily be foreign nationals, as cybercrime is transnational and there is no need for physical proximity.[19] On the other hand, nationality is not a quality attributable to data. It is an attribute of an individual person; therefore, the need to connect individual persons – e.g. a perpetrator – to sought-after data is yet to be fulfilled. Nationality as an attribute cannot accomplish that requirement.

3.1.3 Models from maritime and space law?

Although composed of machinery and millions of miles of cable infrastructure physically tied to different territories all around the world, many describe the Internet as a truly transnational medium denying any bounds and borders, thus forming a space distinguishable from physical territories;[20] the very same comprehension are strongly reflected in the wording "cyberspace". Based on this understanding of a global cyberspace, it seems reasonable to extend the search for comparable legal models to maritime and space law. Both the high seas and outer space are subject to international law and treaties instead of the principle of territoriality to determine jurisdiction. Under the conditions of cloud computing, the loss of location leaves data in the clouds in the same non-territorial state where things on the high seas and in outer space are.

Aboard ships and spacecraft, the flag principle applies, which has been dismissed above as insufficient to deal with the specific problems of investigations in cloud computing environments.[21] International treaties regulating the exploration and use of outer space, the liability for damages and the return of astronauts etc.[22] do not

[17] See *Ambos, Kai*, Internationales Strafrecht, Munich, 2nd ed., 2008, pp. 36 – 46 for more on the principle of nationality.
[18] See Article 22 paragraph 1 lit. d of the Convention.
[19] See *Brenner, Susan W.*, „Cybercrime Jurisdiction", loc. cit., p. 194.
[20] See for example *Rossnagel, Alexander*, „Weltweites Internet – globale Rechtsordnung?", Multimedia und Recht (MMR), issue 1 (2002), pp. 67 – 71 (70).
[21] See above 3.2.1.2.
[22] See e.g. the United Nations Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (General Assembly resolution 2222 (XXI), annex) - adopted on 19 December 1966, opened for signature

explicitly provide for criminal jurisdiction besides the flag principle, which in space is tied to the registration state of space objects where crimes occur rather than to flags.[23] Additionally, the International Space Station Agreement specifies in Article 22 that criminal jurisdiction within the ISS – currently the only manned station in outer space that is not a spacecraft – shall be determined partly by the flag principle (referring to the state of registry of each component) and partly by the principle of nationality, as states are supposed to consult each other and reach an agreement on criminal jurisdiction in case a national of one ISS partner state inflicts damage on a national of another ISS partner state. Unfortunately, and probably due to the rare likelihood of such an event, there are no regulations to be found dealing with criminal procedure and jurisdiction for crimes committed outside ships, space stations or spacecrafts[24]. Therefore, maritime and space law does not provide for a model solution to cover the loss of location in cloud computing other than the previously examined principles.

3.2 An approach beyond territoriality

As neither the existing solution of access with consent nor general principles of international law measure up to the specific challenge created by the loss of location, it's time to ask what would have to be the qualities of an alternative approach to the problem. Based on the findings above, it should be important to choose a legal connecting factor that can be attributed to data and verified before actually accessing the sought-after data. Second, as most states will obviously be very reluctant to accept the (possible) exercise of foreign coercive measures within their sovereign territory, an alternative approach should concentrate on procedural measures that do not involve coercive powers. And finally, conditions and safeguards should be considered, e.g. to restrict such measures to exigent cases[25] and to ensure that the fundamental rights of suspects and third parties are respected properly.

3.2.1 Power of disposal as legal connecting factor

A legal connecting factor that meets the criteria mentioned above can be found in the power of disposal. The formal power of disposal connects any data to the person or persons that obtain sole or collaborative access and that hold the right to alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever. The formal power of disposal is also recognized as legally protected interest of Article 2 (Illegal Access) and Article 4 (Data Interference) of the Budapest Convention on Cybercrime. It therefore not only represents a well-known and manageable legal parameter, but – being a parameter of informatics as well – can actually be used to tie procedural measures to certain files, accounts or any other individual group of data. Last but not least, it is completely detached from location parameters of any kind.

---

on 27 January 1967, entered into force on 10 October 1967; the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (resolution 2345 (XXII), annex) – adopted on 19 December 1967, opened for signature on 22 April 1968, entered into force on 3 December 1968; and the Convention on International Liability for Damage Caused by Space Objects (resolution 2777 (XXVI), annex) – adopted on 29 November 1971, opened for signature on 29 March 1972, entered into force on 1 September 1972.

[23] See *Hermida, Julian*, „Crimes in Space", Annals of Air and Space Law, Vol. XXXI (2006), pp. 1 – 19 (6).

[24] See *Meyer, Alex*, Straftaten im Weltraum, Thessaloniki, special reproduction, 1966, pp. 3 – 22.

[25] This has been suggested by way of an exception to the principle of territoriality, see *Schwerha IV, Joseph J.*, Project on Cybercrime discussion paper, January 2010, loc. cit., p. 18, citing also *Sussmann, Michael A.*, „The Critical Challenges From High-Tech And Computer-Related Crime At The Millenium", loc. cit., p. 470 – 471.

However, using the formal power of disposal as legal connecting factor in a manner that allows for verification and steers clear of the need for coercive measures toward cloud computing providers necessitates an intermediary object which can function as an identifying key. Typically, access to computer data requires authenticating credentials, e.g. combinations of usernames and passwords. This is especially true for cloud computing services, since providers have to store data of millions of users separately while having to maintain allocation. Therefore, authenticating credentials are perfectly suited to serve as intermediary object that can be subject to measures defined by law.

A regulation based on the power of disposal approach might then stipulate that access to stored computer data is possible regardless of where the data is located, if certain cumulative requirements are met, e.g.

- the location of the sought-after data has to be unknown or at least uncertain due to the use of cloud computing technology (which should be replaced by a short yet precise definition);
- access can be established by the sole usage of proper authenticating credentials;
- those very credentials have to belong to or be used by a suspect;
- the credentials have to be obtained in a lawful manner;
- no help from the cloud computing provider is to be sought;
- the suspect is either physically on the territory of the investigating authority or of the same nationality.[26]

Whether to include access to a third party's accounts by use of that third party's credentials for certain reasons or to go into detail about chain of custody measures might also be debated, but would not be constituent factors for such a regulation. From a practical point of view, a regulation based on the power of disposal approach would enable law enforcement authorities to access a suspect's data within the cloud in a feasible manner. The respective authority would only have to legally obtain the user and password combination and be able to prove that additional requirements are met.

3.2.2 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.[27] 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 Googe Mail account, for example, would infringe the right to telecommunication secrecy provided in Germany by Article 10 paragraph 1 of the German Constitution (Grundgesetz, GG). If done in a covert manner instead of openly, such an infringement usually requires a judge's decision beforehand.

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

[26] These references to the traditional territorial and active personality principles of general criminal jurisdiction might prove useful in reaching a consensus on establishing such a measure.
[27] One could consider limiting the scope of this provision to conduct as defined in articles 2 to 9 of the Budapest Convention as well as serious offences committed by means of a computer system.

- 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;[28]
- stipulating obligations to mark the data that has been obtained, accompanied by scheduled deletion obligations.

If established within the framework of the Budapest Convention on Cybercrime, the aforementioned conditions and safeguards would be covered by the Parties' commitment to Article 15 of the Budapest Convention, which states:

> Article 15 – Conditions and safeguards
>
> 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

4 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 de lege ferenda.

---

[28] Notifying the state affected by such a measure, however, seems inappropriate, as the exact location of data gathered as evidence often will still be unknown after it has been accessed.