Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution

Dan Jerker B Svantesson
Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution

Dan Jerker B Svantesson*abcd*

Keywords: law enforcement; electronic evidence; cloud evidence; Mutual Legal Assistance (MLA); cloud providers; Internet jurisdiction; provision of data to law enforcement; evidence; data storage

1. Introduction

Where a law enforcement agency (LEA) seeks access to evidence stored in the ‘cloud’, several interests and considerations need to be balanced. Exactly what those interests and considerations are depend in part on what mechanism the LEA utilises. It also depends on whether the cloud provider in question is domestic or foreign.

Where the data sought is held by a foreign cloud provider, the LEA seeking access to that data has, as noted by Walden, four possible courses of action. Such an LEA may (1) seek the assistance of the relevant foreign LEA via formal Mutual Legal Assistance (MLA); (2) seek informal assistance from the relevant foreign LEA; (3) seek the assistance of the foreign cloud provider; or (4) seek direct access to the data. It is the third of these four options I will focus on exclusively here. Obviously, much can be done to improve the MLA system, and improving that system will affect the need for

---

* Faculty of Law, Bond University
Gold Coast, Queensland, 4229
Australia
E-mail: Dan_Svantesson@bond.edu.au

1 The term ‘cloud provider’ is admittedly not ideal but is here intended to refer to a range of Internet actors, such as social media, email providers and data storage, holding user data in cloud arrangements.


3 ibid.

alternative means of access. But looking at the current forecast for MLA improvements, it would be naïve to think that improving the MLA system would render the alternative means of access unnecessary. Indeed, catering for one or several of the alternative means of access could take some of the burden of the MLA system, which on its own could improve the functioning of the MLA system. Thus, the discussion below is necessary whether or not we also manage to improve the MLA system as such.

My aim is to map out the interests and considerations that need to be taken into account in the pursuit of a framework (whatever form it may take) for facilitating appropriate LEA access to evidence via direct contact with cloud providers while still safeguarding the rights and interest of individuals, as well as the rights and interest of the cloud provider, and those of other states.

2. The variables and the possible scenarios they create

The task outlined above is not an easy one. And it is made more complex by the fact that situations falling into the third category outlined above are characterised by diversity rather than homogeneity. For example, amongst the scenarios where an LEA seeks the assistance of the foreign cloud provider, we need to (1) distinguish between direct requests to the mother company and indirect requests that go via national subsidiaries. Further, we are also required to (2) distinguish between, on the one hand, access sought on an entirely voluntarily bases, and access based on court orders on the other hand. In addition, amongst the latter category we find different types of instruments such as warrants and subpoenas. Finally, all these scenarios must, as was hinted at above, be kept separate from situations where an LEA seeks access to data from a domestic cloud provider, such as where the US government seeks access to data directly from eg Microsoft, Google or Facebook. And also within this category, we can imagine a diversity of scenarios. Thus, we have to, for example, (3) distinguish those situations where the data sought relates to a citizen of the state of the LEA from situations where the domestic cloud provider is asked to provide data relating to a foreign national. In addition, within this category we also must (4) distinguish between situations where the data held by the domestic cloud provider is actually held domestically and situations where the data in question, while held by a domestic cloud provider, is held in another country.

Summarising the above, I have already hinted at six variables: (1) the country of the LEA, (2) the country of incorporation of the cloud provider, (3) the existence of subsidiaries in the country of the LEA, (4) the nationality of the person to whom the data relates, (5) the manner in which access is sought and (6) the location of the data (to the extent ascertainable). To this, we may usefully add, at least, the following variables: (7) the nationality of the suspect(s), (8) the nationality of the victim(s), (9) the location(s) of the suspect(s) at the time of the crime, (10) the location(s) of the victim(s) at the time of the crime, (11) the habitual residence of the suspect(s), (12) the habitual residence of the victim(s) and (13) the availability of alternative means of gaining access to the data, such as via MLA. Furthermore, in some situations, we also need to consider (14) the nationality of the witness(es) whose data is sought, (15) the habitual residence of the witness(es) as well as (16) the location of the witness(es) whose data is sought. Anyone setting out to construct a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers must take account of this diversity of variables and decide whether to cater for all the scenarios they make possible, or whether to adopt a narrower scope.

3. A proposed method

Despite this diversity, certain generally applicable interests and considerations can be identified. To map out those interests and considerations I will here apply parts of a 10-step research method I developed and published some years ago. Under this research method, the first four steps can be viewed as the analytical phase of the method, with step one involving defining the problem. Step two seeks to identify any constraints that fundamentally impact on the issue. For example, if one is to find a solution to the regulation of Internet defamation, one cannot ignore the human right of free speech – the human right of freedom of expression is a fundamental constraint for any solution to the regulation of Internet defamation. The researcher can then move on to identifying other, less significant, constraints that should be taken account of. We can call them non-fundamental constraints. Once all the constraints have been identified, it is necessary to assess how the constraints interact. For example, some constraints will strengthen each other, while others will be each other’s opposites requiring careful balancing from the researcher. In this context it must be realised that, while certain constraints are fundamental in nature, it does not mean that they are absolute. In other words, the observation that the human right of freedom of expression is a fundamental constraint for any solution to the regulation of Internet defamation does not mean that the right of freedom of expression is absolute and may never be interfered with at all.

Applied correctly, steps two (the identification of fundamental constraints), three (the identification of non-fundamental constraints) and four (the assessment of how the constraints interact) ensure that the method takes account of the context of the problem sought to be addressed, thereby disposing of one of the traditional criticisms of stricter doctrinal research methodologies.

The next phase (steps five to seven) – the information gathering phase – is doctrinal in nature and involves an examination of how the problem has been addressed so far (step five), an examination of how similar problems have been addressed so far (step six) and then a critical evaluation of the approaches identified (step seven).

In steps eight, nine and ten (the third and last phase— the construction phase), the researcher must construct the solution (step eight), and then test it against the fundamental, and non-fundamental, constraints (step nine), as well as against any relevant likely future technological developments and uses (step ten). Steps nine (testing the solution against the constraints) and ten (testing the solution against any relevant likely future technological developments and uses) work to ensure that the solution serves the purposes it was intended to serve and has the effects it ought to have when put in the context it will operate.

4. The scope of this article

For the purpose of what I am aiming to undertake here, I will largely restrict myself to steps one, two and three. Thus, my aim here is limited and rather modest. However, I envisage that the research model outlined above may fruitfully be applied for the larger task of actually designing a framework – whether as a voluntary code of conduct or a binding international agreement – facilitating appropriate LEA access to evidence via direct contact with cloud providers. In that sense, what I am doing here

---


6 William Twining, ‘Academic Law and Legal Development’ in Taylor Lectures 1975 (University of Lagos Faculty of Law 1976) 20, as found in Terry Hutchinson, Researching and writing in law (3rd edn, Lawbook 2010) 22.
may be seen as taking those critical first steps of a longer, indeed much longer, journey. I say critical first steps because they set the direction for all the coming steps to be taken.

5. **Step one – framing the research question**

The above has already brought us into the position of framing the research question. The goal should be to construct a framework (whatever form it takes) for facilitating appropriate LEA access to evidence via direct contact with cloud providers while still safeguarding the rights and interest of individuals, as well as the rights and interest of the cloud provider, and those of other states.

In order to be successful, such a framework needs to be developed through a dialogue with a range of parties including governments, cloud providers, LEA, international organisations with relevant expertise (eg the Council of Europe) and academics with relevant insights. The process will be difficult, but the topic is of such fundamental importance that it should not be put off any longer.

6. **Step two – fundamental constraints**

The fundamental constraints that step two of the method invites us to identify are constraints of such fundamental importance to the research task defined in step one that a solution that does not take account of them simply cannot be accepted. In other words, they represent the limits to any acceptable solution.

The constraints discussed here come in at least three different, but partly overlapping, forms. There are practical constraints, such as technical and legal realities, regulatory constraints, such as applicable law that must be taken into account, and aspirational constraints, such as constraints justified by reference to societal goals.

I argue that we can identify, at least, 25 such fundamental constraints (discussed below in no particular order and at varying depth as required), and by mapping them out, we are one step closer to being in a position to start constructing a sensible framework facilitating appropriate LEA access to evidence via direct contact with cloud providers while still safeguarding the rights and interest of individuals, as well as the rights and interest of the cloud provider, and those of other states.

Alternatively, for anyone who has already embarked on the journey towards designing a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers, the fundamental constraints outlined here may serve as a useful checklist to assess the work they have done so far. In any event, in an ideal world the exercise of outlining the fundamental constraints should merely result in a list stating the obvious. However, due to inevitable subjectivities, that is, of course, not always so.

Against that background, here is my proposed outline of the fundamental constraints we need to consider if we are to construct a framework (whatever form it takes) for facilitating appropriate LEA access to evidence via direct contact with cloud providers while still safeguarding the rights and interest of individuals, as well as the rights and interest of the cloud provider, and those of other states:

**Cloud providers have a duty to be good world citizens so as to help legitimate law enforcement actions.** The strength of this duty is partly dependent on the degree of connection between the cloud provider and the state of the LEA, as well as on the degree to which the state of the LEA’s has a legitimate interest in the matter to which the data relate. Further, the strength of this duty is also partly dependent on the strength of the LEA state’s jurisdictional claim (as assessed under the LEA’s
domestic law, as well as under international law) over the suspect. Finally, as is hinted at in the reference to *legitimate* law enforcement, the strength of this duty is partly dependent on the type of crime being investigated (eg child abuse should concern everyone) and partly dependent on the law enforcement process of the state of the LEA.

**Cloud providers have a duty to be respectful of the human rights (such as privacy) of their users.** This duty is unquestionable and stems from a range of human rights treaties, such as the International Covenant on Civil and Political Rights, and in the context of Europe, the European Convention on Human Rights (ECHR) and the Charter of fundamental rights of the European Union with its specific protection of personal data. This matters in assessing whether, and to what degree, to assist LEAs. This also matters in assessing how to deal with information received by LEAs that seek information.

**Cloud providers have a duty to be respectful of the human rights (such as privacy, reputation, victims of crime etc) of non-users.** Also this duty stems from human rights treaties and is equally unquestionable. This matters in assessing whether, and to what degree, to assist LEAs. This also matters in assessing how to deal with information received by LEAs that seek information.

**Cloud providers cannot comply with conflicting duties.** Such conflicts are unfruitful, harmful and should be avoided. And where they cannot be eliminated, the option of providing cloud providers with immunity or other forms of protection (such as so-called ‘clawback’ statutes) should be considered.7

The idea of territorial sovereignty in an absolute sense does not fit with our interconnected world characterised by constant and fluid cross-border interaction. A state cannot expect to have exclusive jurisdiction over all data that happens to sit on a server in its territory simply for the reason that it happens on its territory. It is already well established that jurisdiction does not necessarily extend to transitory data, and in our cloud computing world, the distinction between transitory data and data stored on a server in a country is not a sharp one. Further, the territoriality thinking is binary—either something happens on a state’s territory or it does not—but the legitimacy of jurisdictional claims is not binary, they are always a matter of degree. Thus, we will not find any good solutions to the matter of LEA access to evidence via direct contact with cloud providers by focusing on territoriality. We should abandon the territoriality principle as the core of our thinking on jurisdiction and replace it with a test that recognises the concerns above. For example, elsewhere I have proposed the following as the jurisprudential core of our thinking on jurisdiction:

*In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:*

1. *there is a substantial connection between the matter and the State seeking to exercise jurisdiction;*

2. *the State seeking to exercise jurisdiction has a legitimate interest in the matter; and*

3. *the exercise of jurisdiction is reasonable given the balance between the State’s legitimate interests and other interests.*8

---

7 Dan Svantesson, ‘Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries’ (2014) 30 Computer L & Sec Rev 348-56.

This gives us a solid foundation from which we can start building more detailed rules that courts apply and so on.

In approaching the question of jurisdiction, investigative measures cannot be handled under the strict rules governing enforcement jurisdiction. International law typically distinguishes between three types of jurisdiction: prescriptive jurisdiction, judicial jurisdiction and enforcement jurisdiction. A key reason for the current difficulties associated with LEA access to evidence via direct contact with cloud providers is found in the fact that such investigative measures are seen to fall into the category of enforcement jurisdiction – the type of jurisdiction most tightly bound up by the territoriality principle. To make progress we need to recognise that LEA access to evidence via direct contact with cloud providers falls into a previously overlooked fourth category of jurisdiction – what we can call investigative jurisdiction\(^9\) – that can be more relaxed in its relationship to territoriality.

Where a cloud provider enjoys rights in a state to which it has a substantial connection, and where that state has a legitimate interest in the cloud provider (eg the state of incorporation), those rights must be considered when an assessment is made as to whether the cloud provider reasonably should comply with duties, conflicting with those rights, stemming from another country. The relevance of those rights is a matter of degree where the level of substantial connection and legitimate interest must be considered. For example, in the absence of other connecting factors and interest, the state of incorporation and head quarter may enjoy stronger interest in, and connection to, the cloud provider than does the state where the data happens to sit on a server. However, this balance may quickly change if other connecting factors and interest can be established pointing to an overall more substantial connection to, and legitimate interest of, the state where the data sits. In other words, a careful case-by-case balancing act is required.

Different rules are needed for different types of data as the degree of data privacy sensitivity varies. This distinction cannot rely on the binary distinction between personal data and non-personal data typical of data privacy laws. Furthermore, this distinction cannot rely only on the categorisation of subscriber data, traffic data and content data (or the even more inelegant distinction between metadata and data) since the sensitivity of the data may vary amongst data falling into any of those categories. For example, the sensitivity of subscriber data depends on the service to which the information relates.

A distinction between access to stored data and live data is necessary. The difference between access to stored data and access to live data is well established and must be recognised in the discussions.

Digital evidence stored on foreign servers are frequently relevant in relation to completely domestic crimes. The way people use information technology has resulted in a situation where evidence frequently is stored in the cloud even though the criminal activity in question is entirely domestic – a local offender, a local act and a local victim – and the crime is unrelated to information technology as such.

Where fully respected, anonymity – an articulated component of some data privacy frameworks – undermines the identification of factors such as the relevant person’s localisation, nationality and residence. Any framework facilitating LEA access to evidence via direct contact with cloud providers must carefully balance the legitimate calls for anonymous interaction online with competing interest.

Netherlands Presidency of the Council of the EU Debriefing Conference on Jurisdiction in cyberspace (7-8 March 2016, Amsterdam) doc. 7323/16.

Cloud providers must be transparent as to how many requests for access they get, from where those requests originate, what those requests relate to, how many requests result in access being granted etc. Several major cloud providers already issue ‘transparency reports’ outlining this type of information.

Cloud providers need to be transparent in their terms of use as to how they interact with LEAs, including how they treat the information they receive as part of access requests. For example, as to when data is voluntarily disclosed, when disclosed upon request, when disclosed due to court order etc. To a degree, but only to a degree, user expectations can be managed this way. However, we must be mindful that users rarely read and understand the terms of use. In addition to these useful resources, we must ensure that any framework contains mechanisms to control how cloud providers use the – sometimes very sensitive – data they are provided as part of the request. For example, we want to avoid a situation where cloud service users receive targeted advertisement for lawyers specialising in particular fields corresponding to the request cloud providers receive from LEAs.

Cloud providers need to be transparent in informing the affected user where data is in fact communicated to LEAs, unless there are strong reasons not to inform the user. In identifying when a user should not be informed, we can draw upon existing laws addressing this matter.

The urgency of data access will vary from case to case. Emergency access procedures must be put in place for certain clearly defined and delineated situations.

Individuals have an interest in their data privacy rights. As is clear from international human rights law, these rights are fundamental but not unrestricted.

Individuals have a general interest in crimes being detected, investigated, prevented and solved, and in that criminals are punished. This interest is rooted in the proper functioning of society and exists irrespective of the location from which the crime was committed and irrespective of the location at which evidence necessary to detect, investigate, prevent and solve are found.

Victims of crime have a particular interest in crimes being detected, investigated, prevented and solved, and in that criminals are punished. This interest exists irrespective of the location from which the crime was committed and irrespective of the location at which evidence necessary to detect, investigate, prevent and solve are found.

States have a duty to be good world citizens so as to help legitimate law enforcement actions in other countries. The strength of this duty is partly dependent on the type of crime (eg child abuse should concern everyone).

States have a duty to control activities within their jurisdiction so as to prevent criminal activities originating under their control affecting other states, or the citizens of other states. This duty is a necessity in the international system, not least in order to avoid ‘safe havens’.

States have a duty to be respectful of the human rights (such as privacy, reputation, victims of crime etc). Again, this indisputable duty is founded on international human rights law.

It is not always possible to ascertain the geographical location of the server on which data is hosted. This undermines the usefulness of current rules attributing significance to the location of the data as a determining factor in the assessment of whether LEAs should be provided access to the data.

In the context of cloud computing, data is frequently distributed over more than one server, either as duplicates or simply by the fact that it is broken into small parts. This undermines the usefulness of current rules attributing significance to the location of the data as a determining factor in the assessment of whether LEAs should be provided access to the data.
Appropriate procedural safeguards ensuring legitimacy of data request must be established. Such procedural safeguards cannot be based on vague references to human rights standards as these standards are neither sufficiently clearly defined nor universally agreed upon. Furthermore, what amounts to ‘due process’ in the context of LEA access to evidence via direct contact with cloud providers must be identified in detail.\(^\text{10}\)

The proper substantive rules, scope, structure and nature of any framework for facilitating appropriate LEA access to evidence via direct contact with cloud providers depends on the countries to be covered by the framework. The reality is that different countries have very different attitudes towards matters such as human rights and due process. And in light of this, it must be concluded that not all countries have reached a stage of maturity making it suitable for their LEAs gaining access to evidence via direct contact with cloud providers in other countries. Thus, while we must aim to make our solutions of today scalable to the world of tomorrow, where hopefully many more countries can join the framework, we do not need to try to construct a solution that caters for request from countries failing to meet appropriate human rights and due process standards.

All these 25 fundamental constraints must be taken into account when we design a framework for facilitating appropriate LEA access to evidence via direct contact with cloud providers. Failure to do so will automatically render the solution unacceptable.

### 7. Step three – non-fundamental constraints

To all this we should, as per step three, add the relevant non-fundamental constraints. Like the fundamental constraints, the non-fundamental constraints come in at least the three different forms of practical constraints, regulatory constraints, and aspirational constraints. At any rate, amongst them we find at least the following:

1. It is easier to build on existing instruments (eg the Council of Europe’s Budapest Convention on Cybercrime) than it is to build from scratch;
2. Initial consensus is best sought within a group of countries with similar legal approaches and amongst which there is a certain degree of trust in LEA cooperation. The EU is an obvious candidate in light of its relative existing harmonisation (and given that many of the data privacy constraints will stem from the EU);
3. Rules for LEAs should reasonably be different to the rules for intelligence services;
4. Balkanization incurs a cost, a financial cost for intermediaries, and at least an efficiency loss for users;
5. While perhaps unsurprising in the current climate, unilateral action by LEAs to gain direct access to data from cloud providers is unsuitable as a long-term strategy;
6. The efficiency of the actual cooperation between LEAs and intermediaries will always, in part, depend on the extent to which a ‘culture of cooperation’ is developed;
7. Harmonisation of substantial law, while useful, is not likely in the short term, and thus procedural laws must be coordinated;

8. It would be appropriate to include limitations as to what type of crimes ought to be covered by the framework allowing LEA access to evidence via direct contact with cloud providers. First, from a practical perspective, this will help limit the number of requests. Second, given the privacy concerns involved, it seems reasonable to conclude that not all alleged crimes are of such importance as to make legitimate the relatively intrusive step of giving LEA access to evidence via direct contact with cloud providers; and

9. The manner in which information is acquired may impact its value when presented as evidence in courts.

8. Concluding remarks

It is perhaps unsurprising that civil rights activists and LEAs view the discussed matters from different perspectives. But having spoken at events on both sides of the Atlantic on the topic addressed here, I have also witnessed great cultural differences in how various stake-holders view the relevant considerations – and how these considerations should be balanced. There also seems to be a disconnect between the various initiatives taken in this arena in Europe and the US. If a solution with potential for long-term success is to be found, we necessarily must map out and agree upon what are the relevant considerations. The above has all been aimed at this first step.

If the fundamental constraints outlined above are accepted as an appropriate description of these considerations, stake-holders should proceed to enter into a dialogue as to how these considerations ought to be balanced; because one thing is certain, insisting on absolute privacy protection or unfettered LEA access to any data they see fit to request will get us nowhere. And if we fail to find appropriately balanced solutions, we should not expect a status quo to be maintained. LEAs have demonstrated a clear appetite for unilateral action, and such actions have been sanctioned by the highest courts. This appetite is likely to increase rather than decrease. As noted, unilateral action by LEAs to gain direct access to data from cloud providers is unsuitable as a long-term strategy.

In the above, I have also pointed to 16 variables that anyone setting out to construct a framework facilitating appropriate LEA access to evidence via direct contact with cloud providers must take into account; either by making sure that their proposed frameworks actually cater for the rich diversity of scenarios those variables make possible, or by adopting limitations narrowing the scope of their proposed frameworks.

And if I may finish with my ‘pet concern’, insisting on some outdated 17th century notion of territoriality will only provide us with poor outcomes that serve none of the interests involved in the debate about LEA access to evidence via direct contact with cloud providers.

Acknowledgements

In writing this paper I have benefitted greatly from speaking, and getting feedback, at Crossing Borders: Jurisdiction in cyberspace, Dutch EU Council Presidency (The Netherlands) (March 2016) as well as at the ‘Jurisdiction and Extraterritoriality in a Connected World’ session at RightsCon in San Francisco (March 2016).

References

Danish Supreme Court Order delivered on Thursday 10 May 2012 (Case 129/2011)


Netherlands Presidency of the Council of the EU Debriefing Conference on Jurisdiction in cyberspace (7-8 March 2016, Amsterdam) doc. 7323/16


Svantesson D, ‘A legal method for solving issues of Internet regulation’ (Autumn 2011) 19(3) Intl JL & Info Tech 243

Svantesson D, ‘Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries’ (2014) 30 Computer L & Sec Rev 348


Twining W, ‘Academic Law and Legal Development’ in Taylor Lectures 1975 (University of Lagos Faculty of Law 1976) 20, as found in Terry Hutchinson, Researching and writing in law (3rd edn, Lawbook 2010) 22
