Crime and Criminal Investigation in the Clouds
Threats and Opportunities of Cloud Computing for Dutch Criminal Investigation

Bert-Jaap Koops, Ronald Leenes, Paul De Hert & Sandra Olislaegers

This is a summary of a Dutch report, commissioned by the Netherlands Ministry of Security and Justice. The report, B.J. Koops, R. Leenes, P. De Hert & S. Olislaegers (2012), *Misdaad en opsporing in de wolken. Knelpunten en kansen van* cloud computing *voor de Nederlandse opsporing*, Tilburg/The Hague: TILT/ WODC, October 2012, is available at http://english.wodc.nl/publicaties/.

Summary

Background and research question

Cloud computing refers to outsourcing data management or computer applications to a service provider, in which data are stored across various servers, often without control over the exact location of the data. 'Typical' cloud computing examples are email services such as Gmail and Hotmail, data storage or sharing services such as DropBox and Megaupload, application services such as Google Docs, and development platforms such as Amazon AWS. Cloud computing is expected to become an important part of the Internet landscape. This results in shifts in data-processing and data-storage patterns, which essentially amount to data no longer being stored on business premises or with people at home, but elsewhere. This can involve vulnerabilities, both for companies and citizens who hand over control over their data, and for law-enforcement agencies who, in practice, strongly rely on local investigations of data. Thus, cloud computing has the potential to profoundly impact the committing of data-related crimes as well as digital investigations and prosecution of crime.

This gives cause to explore the actual and potential consequences of cloud computing for Dutch criminal investigation and prosecution. This study answers two questions: what are possible problems and opportunities of cloud computing for committing crimes and for investigating and prosecuting crimes in and from the Netherlands? And what are suitable directions for addressing the identified problems and to make the most of the identified opportunities for combating crime?

The research has been executed through desk research, interviews with five Dutch experts, and a small-scale survey among foreign experts.

Crime and substantive criminal law

Legal practice shows as yet few cases of crime in which the cloud played a substantial role. Cloud services are known to be used for storing and exchanging illegal material and for committing botnet attacks, but the cloud is not significantly different from other Internet services in this respect. There seem to be no special aspects that make cloud-related crime substantially different from other forms of cybercrime, in terms of substantive law. The Dutch Criminal Code (DCC) [Wetboek van Strafrecht] seems, for the time being, sufficiently suitable to enable prosecution of crimes committed in or through the cloud.

Two elements do merit further study to determine whether the law should be adapted. First, the legislator could investigate whether the provisions relating to telecommunications service

providers apply, or should apply, to cloud storage providers. As people are entrusting their files to Internet service providers for long periods, not only communications need to be protected but also data entrusted to service providers in general. It would seem plausible to extend article 273d DCC (which penalises telecoms providers if they inspect the content of data entrusted to them) so as to include storage providers.

Second, the legislator could assess whether the cracking of passwords and encrypted files – which is facilitated by the computing power of cloud infrastructure services – is sufficiently endangering as to merit specific criminalisation. An alternative could be to rely on self-regulation by cloud providers, and to use as a safety net the existing provisions, such as hacking and fraud, that penalise the misuse (rather than the cracking) of passwords.

Criminal investigation in the cloud

Experiences with cloud computing in investigation and prosecution practice seem to be scarce to date, both in the Netherlands and abroad. The only exception are web services, which have existed for a longer time and which regularly feature in criminal investigations. Still, cloud computing is expected to create considerable challenges for investigation in the foreseeable future.

First, the statutory framework raises some legal questions and impediments. It is unclear when exactly a cloud provider will qualify as a communications provider or a public telecommunications provider. Moreover, the Dutch Code of Criminal Procedure (DCCP) [Wetboek van Strafvordering] distinguishes between stored data and data in transit, and between communication and non-communication. These distinctions are sometimes hard to apply in the case of cloud storage and processing services; they also seem to become less relevant. Besides, the rise of cloud computing, along with an increasing deployment of encryption, reinforces the question – which is already being discussed – whether a power should be introduced for the police to covertly acquire remote access to (i.e., to hack into) computers of suspects.

Second, investigation practice will have to adapt in order to meet the shift of data storage from hard disk to cloud. In searches, the police will have to be more aware of the importance of searching and seizing computers while they are active, in order to secure the computer's temporary memory and activated network connections, including connections with cloud services. Classic searches and classic wire interceptions will gradually have to make room for Internet interceptions – something which legislation and legal practice are not yet very well catering for.

Third, and most importantly, the most prevalent methods to collect digital evidence (searches, production orders, intercepting data) have limited effect with data that are stored in, or exchanged through, the cloud. The main bottleneck is the territorial boundaries to which Dutch investigation is still bound. Since cross-border network searches are not allowed (except in the rare cases of having permission from the suspect or voluntary co-operation by foreign service providers), law enforcement has to rely on mutual assistance with an order for foreign cloud providers to produce data. This is not something new: cyber-investigation has traditionally suffered from having to deal with questions of cross-border access to data. However, these questions become much more profound through the 'loss of location' that the cloud implies. Files are usually stored in the cloud among different servers, in multiple copies and carved in pieces; the system itself calculates, on the basis of demand and supply, the most efficient storage and continuously moves around file pieces accordingly. This makes it very hard to determine, also for the cloud provider itself, on which exact location(s) a file is actually stored. The location where data 'are' no longer works as the main clue for determining rights and duties in relation to the cloud.

For investigation practice, the loss of location is particularly relevant, especially given the context of criminal procedure law, in which territorial sovereignty continues to play a very dominant role. When criminals migrate their data management to the cloud, Dutch investigation practice will run into the wall of territorial limitations. Both law and public policy will have to start

addressing this problem. The Netherlands will have to invest in co-operation, both with foreign governments and with service providers. Further streamlining of mutual-assistance procedures is essential for cloud investigations.

The loss of location provides a more fundamental challenge as well, as it also impacts on the abstract level of jurisdiction and sovereignty theory. One can roughly distinguish two schools of thought: 'territorialists', who emphasise the physical location of servers and routers, and 'cybernauts', who argue that physical locations are only accidental in cyberspace. The territorialists may have to cede ground to the cybernauts, once cloud computing captures an established place in the Internet landscape. That would be in line with literature about the cloud, which seeks to establish jurisdiction based on the persons who have lawful access to data (such as providers and customers) rather than on the location of the server that hosts data.

This implies as well that the cloud challenges the classic criminal-law regulatory model of mutual assistance. There is a need to reflect on the role of sovereignty in criminal investigation. Partly because of the difficulty of determining the location of data in the cloud, and partly because investigation in the cloud sometimes calls for more expeditious action than mutual assistance – however streamlined it may be – can offer, there is good reason to allow a cross-border network search. The Belgian model, in which network searches can, under certain conditions, be extended to foreign network connections with *ex post* notification to the foreign state at issue, could serve as a source of inspiration. Another question is under which conditions the Netherlands would consider it justified for law enforcement to contact foreign providers directly instead of walking the path of mutual legal assistance. Both issues can obviously only be addressed on the basis of reciprocity: the Netherlands could be allowed to collect data from abroad only if foreign countries could do the same on Dutch territory. In this manner, a new and modern meaning could be given to sovereignty in a networked world order.

Prosecution and the cloud: forensic aspects

Besides impediments in investigation, obstacles may also arise in the prosecution stage if the reliability of cloud-originating evidence can be contested in court. Standards and procedures for gathering evidence from the cloud remain embryonic and have not yet been tested in legal practice. Technical and, to some extent, also legal risks pertain to material that is provided voluntarily or upon court order by foreign cloud providers.

Technically, it is not easy to prove that a document downloaded from the cloud is the same as the document that was uploaded into it, because of the distributed and automated dynamic storage. It will not always be evident which forensic procedures a cloud provider has followed to obtain a document; frequently, technical features necessary for forensic investigations (such as logging and audit trails) are lacking in current cloud infrastructures. Consequently, there is a need to develop standards and procedures, as well as to closely collaborate with cloud providers to build in basic features for forensic investigations in cloud infrastructures and practices.

From a legal doctrinal point of view, not many complications in cloud evidence should be expected in the Netherlands. Evidence obtained from abroad can be used as such. Occasionally, if the defence contests the admissibility or reliability of cloud-originating evidence, the prosecution may have to substantiate its lawfulness and reliability. Whether that will cause significant problems – more than in other cases of digital evidence – is something that practice will have to show.

Opportunities

Although our research sources are largely focusing on threats, the cloud may also offer opportunities for investigation and prosecution, in three areas. The main opportunity is that the migration of data from the suspect's hard disk to the cloud enables the police to covertly investigate a much wider range of data, without a physical search of his computer alerting the

suspect that he is being investigated. Through Internet interception or a production order addressed to the cloud provider (with a secrecy or gagging order) data can be investigated that formerly could only be collected by searching the hard disk (which usually is under direct physical control of the suspect). This allows preliminary investigations to continue for a longer period, which can have tactical advantages in certain cases. However, this opportunity can only be exploited if the problems of cloud investigation are addressed, including notably impediments of Internet interception and of 'location-based' investigation practice.

The other areas offering potential opportunities are the cloud's computing power, which law enforcement could utilise for instance to crack encrypted files, and in the cloud's storage capacity, which could offer a cost-efficient solution for the ever increasing amounts of data that law enforcement are retaining. Capitalising on computing power concerns a relatively uncontroversial part of police practice that could be employed without much ado, but using cloud storage capacity for police data is a complex issue that requires further reflection. More research and a complex policy trade-off are required to determine whether the potential savings in costs outweigh the manifold risks of storing police data in the cloud.

Conclusions and directions for addressing problems

Cloud computing as such does not create fundamentally new consequences for investigation and prosecution. It does raise some questions on how to apply criminal law and criminal procedure law, but these are questions that fit easily in the regular maintenance of cybercrime legislation that is necessary to perform in any case. Nevertheless, the shifts caused by cloud computing could still make a considerable difference. Upon further scrutiny, the rise of the cloud does have important effects, because the migration of data processing to the cloud compounds existing developments and problems. Primarily, the 'loss of location' fundamentally challenges the territorial orientation of law enforcement. This challenge should be met at the levels of legislation, policy, and practice.

The legislator should reconsider the legal framework's system in substantive and procedural criminal law in relation to Internet providers, such as the scope of the concepts of 'communications provider' and 'telecommunications provider' and the distinction between stored data and data in transit. Also, when revising article 13 of the Dutch Constitution [Grondwet], the legislator should take cloud services into account when determining the new focus and boundaries of the secrecy of correspondence. The legislator could contemplate the adequacy of certain investigation powers to gather data from the cloud as well. For example, in relation to the domestic network search (art. 125j DCCP), is it justified to have different levels of legal protection in searches of vehicles, non-residential places, and dwellings (art. 96b, 96c, 97/110 DCCP), given that cloud data can be accessed from any device in any place? Similarly, attention should be paid to the legal impediments in Internet interception, which relate to, among other things, reporting requirements, privileged information, and *ex ante* selection of data. Finally, the cloud compounds the current question whether and, if so, under which conditions, a power should be created for covert remote searches, particularly in the form of hacking computers by remotely placing police trojans.

For public policy, the first challenge is to establish barriers that make it harder to commit cloud crime in and from the Netherlands. A barrier model could be developed for cybercrime, taking into account the opportunity structure of the cloud, in which possible interventions – focusing on criminals, citizens, industry, Internet providers, and government – are identified for each step that is involved in the committing of a (cloud-related) cybercrime. A second policy area is cloud security. Stimulating cloud security fits well in the broad cybersecurity policy, particularly if a substantial migration is going to take place of critical forms of data processing to the cloud and, consequently, the cloud would acquire the character of a vital infrastructure. Cloud security should therefore feature high on the agenda of the National Cyber Security Council. Third, public

policy faces the challenge of developing a strategy to learn to live with the 'loss of location'. This implies not only investing in co-operation with foreign governments and cloud providers, but also, and crucially, to reconsider the meaning that the Netherlands wants to give to sovereignty in a networked society. The classic criminal-law model to do everything through mutual legal assistance will increasingly run into its own limitations. The Netherlands should determine how far they want to go in cross-border collection of data, along with a reciprocity-based willingness to allow foreign authorities to access data stored in the Netherlands.

For law-enforcement practice, as long as the legal impediments – including the territorial restrictions – have not been removed, the challenge will be to make the most of current investigation powers with all their limitations, and to learn to better utilise computer and network searches and Internet interception. Generally, law enforcement will have to continue walking the orthodox path of mutual legal assistance. In exceptional and urgent cases – when legal assistance does not function well enough – practice could perhaps experiment with non-orthodox measures. Transparency and accountability are crucial requirements in experimental cases, so the activities can be tested in court and thus help in further developing legal doctrine. Non-orthodox measures in cloud investigations, including those that only yield intelligence rather than evidence, should therefore always be accounted for in the criminal file. This will also emphasise the urgency for legislators and policy-makers to come up with better supranational regulation of cross-border data collection in the era of cloud computing.

In sum, we can conclude that for the time being, cloud computing offers more impediments than opportunities for the investigation and prosecution of crime. However, legislation, public policy, and legal practice can make a virtue of necessity if they manage to take up the gauntlet and devise a new, systematic, and balanced regulatory framework and practice for investigating the cloud. Sooner or later, even criminal law doctrine and criminal law practice in an ICT society will have to learn to live with the loss of location. There is much to say for it to be sooner rather than later.