available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Digital evidence and 'cloud' computing

Stephen Mason [a], Esther George [b,1]

[a] Barrister, UK
[b] Crown Prosecution Service, UK

Keywords:
Digital evidence
Cloud computing
PACE
Cybercrime

ABSTRACT

The term 'cloud computing' has begun to enter the lexicon of the legal world. The term is not new, but the implications for obtaining and retaining evidence in electronic format for the resolution of civil disputes and the prosecution of alleged criminal activities might be significantly affected in the future by 'cloud' computing. This article is an exploratory essay in assessing the effect that 'cloud' computing might have on evidence in digital format in criminal proceedings in the jurisdiction of England & Wales.

1. The meaning of 'cloud' computing

The word 'cloud', in cloud computing, is a fairly accurate description of the ephemeral nature of the structure by which the services are offered.[2] Just as a cloud might appear and disappear rapidly, and the forces of air, heat and water vapour will change the internal dynamic of the cloud, so the services offered over the Internet by providers of software can be as equally as transitory. In this article, cloud computing is described by reference to a set of characteristics, rather than by offering a definition.[3] Cloud computing uses the Internet to provide a service. The five essential characteristics mentioned in the definition provided by the National Institute of Standards and Technology (NIST) comprise:

(a) An ability to use the facilities of a computer or number of computers, such as server time and network storage, as required, without the need for human interaction.
(b) The user can use any mechanism to obtain access to the Internet, including computers, mobile telephones, and PDAs.
(c) The entity providing the computing resources will probably include a provision to enable them to determine what happens to data: in time and space. This means the provider may have the ability to send data to any computer anywhere in the world at any time to any entity in order to provide the service to the customer, and the data can be moved around the world to different providers at any time in order to satisfy the rise and fall in demand, or to enable the provider to increase the margin of profit. The customer tends not to have any control over the exact location of the computing resources, although they might be able to

[1] The authors thank Burkhard Schafer, Professor of Computational Legal Theory, School of Law, University of Edinburgh, and Co-director of the Joseph Bell Centre for Forensic Statistic and Legal Reasoning and Alexander Seger of the Council of Europe for their comments on this paper. The views expressed and conclusions reached remain the sole responsibility of the authors.

[2] A paper entitled 'Introduction to cloud computing architecture' (June 2009) by Sun Microsystems provides a useful technical introduction, available at http://www.sun.com/featured-articles/CloudComputing.pdf; also useful is Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing* V2.1 (December 2009), available at https://cloudsecurityalliance.org/guidance/.

[3] One technical definition of cloud computing has been offered by Peter Mell and Tim Grance of the National Institute of Standards and Technology, Information Technology Laboratory:
'Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.'
Version 15 (10-7-09), available at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2011.07.005

specify that data must remain in a specific country or in a particular data centre.

(d) Providers generally claim to have the flexibility to deal with high demand very quickly, with the concomitant ability to continue to offer a service when demand falls.

(e) The service is measured by automatically controlling and making the best use of any resources that are available by distributing data that is appropriate to the type of service, such as the storage of data, the processing of data, the rate of data transfer, and the number of users that are active at any one time.

The transient nature of cloud computing is also reflected in the various business models used to sell the service. They include:

- Cloud software as a service (SaaS), where the customer uses applications provided by the seller. One example that has been in use for some time is web-based e-mail. In this respect, the customer uses the network, servers, operating systems, storage facilities, and possibly individual applications provided by the seller.
- Cloud platform as a service (PaaS), by which the seller provides the infrastructure (network, servers, operating systems, storage facilities) to enable a customer to use their own applications that they create by using any programming languages and tools supported by the seller. The seller will not necessarily offer its own or a single infrastructure to provide the service. It may act as an 'aggregator' by which the seller uses a number of third parties to provide separate applications and sets of hardware, but the buyer is given the impression that that the service they are paying for is one consolidated infrastructure.
- Cloud infrastructure as a service (IaaS) (sometimes called a 'hosted' service), where the seller provides the infrastructure (network, servers, operating systems, storage facilities) to enable the customer to use and run software of their choice, which can include operating systems and applications.

In each of the models outlined above, the underlying infrastructure (operating systems, network, servers, operating systems, storage facilities) is usually in the control of the provider (although not always – the provider may well reserve the right to sub-contract any aspect of the service it provides to any sub-contractor anywhere in the world), although the seller may permit the customer a certain degree of control over selected networking components, such as firewalls, for instance. Each of these service models in turn is controlled and run in a variety of ways, including:

- A 'private cloud', where the infrastructure is operated solely by or on behalf of a single entity. The infrastructure might be owned and managed by the organization; alternatively, it might be owned and managed by a third party on behalf of the entity, and the infrastructure might be physically located in the premises of the organization, or in another geographic location.
- A 'community cloud', where the infrastructure, which might be shared by several organizations, provides facilities to a specific community that has shared interests. The infrastructure might be managed by one or more of the organizations; alternatively, it might be owned and managed by a third party on behalf of an single entity or any number of the entities jointly, and the infrastructure may be physically located on the premises of one of the organizations, or in another geographic location.
- A 'public cloud', where a provider owns the infrastructure and makes it available to anybody that wishes to pay for the service. The way each provider deals with the rise and fall in demand will affect how data is dealt with under this model. In essence, the providers act in a similar way as an electricity grid: they will trade between each other to buy and sell capacity to process data or store data, or both process and store data.
- A 'hybrid cloud', where an infrastructure is formed of two or more cloud infrastructures that in turn can be a mixture of private, community, or public infrastructures. Each infrastructure retains its unique characteristics, and each entity has standard or proprietary technology that enables data and applications to be moved across the infrastructures to facilitate the balancing of the load during periods of high take-up by customers.

For persons reading this article, it will quickly become apparent that people intent on committing crimes might begin to take advantage of the transitory nature of the services offered by cloud computing, thus making it exceedingly difficult for authorities investigating alleged offences to gather evidence in digital format. In addition, an organization might decide to use a form of cloud computing for perfectly legitimate reasons, but find itself in difficulties if it is required to produce evidence in digital format as the result of civil litigation – or a party seeking to establish sufficient evidence of wrong doing before taking legal action might find itself disadvantaged in obtaining a suitable preliminary order to search for possible evidence.[4]

The remainder of this article will discuss, at a high level of generality, some of the possible problems that cloud computing might bring to criminal investigations.

1.1. *The copies of data*

Data may be transferred between many computers across a number of continents during the time a person or legal

[4] In civil proceedings in the USA where data is stored in a cloud computing service, courts have ordered that such data be disclosed if it is relevant to the proceedings, for which see the following examples: *National Economic Research Associates, Inc., v Evans* 2006 WL 2440008 (e-mail communications exchanged between employee and his lawyer sent over a laptop computer owned by the business via the employee's personal web-based e-mail account and protected by a password were the subject of privilege); *Romano v Steelcase, Inc.*, 907N.Y.S.2d 650 (in an action for injuries sustained as a result of a motoring accident, the defendant obtained an order to obtain relevant personal information uploaded by the claimant on the social networking web sites Facebook and MySpace to counter the claim by the claimant that she had had suffered permanent injuries).