COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Can small users recover from the cloud?

Roger Clarke [a,b,c,*]

[a] *Xamax Consultancy Pty Ltd, Canberra, Australia*
[b] *UNSW Law, Sydney, Australia*
[c] *Research School of Computer Science, ANU, Canberra, Australia*

Keywords:
Backup
Recovery
Cloud computing
SaaS
Small business
Consumers

A B S T R A C T

Large numbers of small organisations and prosumers have shifted away from managing data on their own devices and are now heavily reliant on service-providers for both storage and processing of their data. Most such entities are also dependent on those service-providers to perform backups and enable data recovery. Prior work defining users' backup needs was applied to this context in order to establish specifications for appropriate backup arrangements. A sample of service-providers was assessed against those specifications. Their backup and recovery mechanisms were found to fall seriously short of the need.

1. Introduction

All organisations are responsible for managing their data effectively, but only those organisations that are of substantial size are capable of bringing appropriate resources to bear on the problem. The focus of this paper is on entities that lack scale and IT expertise. Further, the paper is concerned specifically with those aspects of data management that relate to data availability and integrity, and that are addressed by backup and recovery arrangements.

1.1. *Small users*

The entities within scope of the paper are of several kinds. One is 'micro-organisations' that involve at most one or two individuals. They may or may not be incorporated, their activities may be stimulated by economic or social motivations, and they may be for-profit or otherwise. Some small organisations, with up to c.20 employees, have similar characteristics.

A further relevant category of entities is individuals who make relatively sophisticated personal use of computing facilities. This may be for the management of personal finance, tax and pension fund, for correspondence, for databases of images, videos and audio, or for a family tree. Such individuals are referred to here as 'prosumers'. The term was coined by Toffler (1970, 1980), and has progressively matured (Tapscott and Williams, 2006; Clarke, 2008). A prosumer is a consumer who is proactive (e.g. is demanding, and expects interactivity with the producer) and/or is a producer as well as a consumer. In the context of computer usage, a third attribute of relevance is professionalism, to some extent of the person themselves but also in relation to their expectation of the quality of the facilities and services that they use.

However, the significance of the work reported in this paper extends beyond micro-organisations and prosumers. During the last two centuries, workers were mostly engaged full-time by organisations under 'contracts of service'. The last few decades have seen increasing casualisation of workforces, with large numbers of individuals engaged through 'contracts for services', giving rise to 'the gig economy'. This requires each

* 78 Sidaway St, Chapman, ACT 2611, Australia.
E-mail address: Roger.Clarke@xamax.com.au.

http://dx.doi.org/10.1016/j.clsr.2017.08.004
0267-3649/

Please cite this article in press as: Roger Clarke, Can small users recover from the cloud?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.08.004

individual to take a far greater degree of self-responsibility. To the extent that large organisations depend on sub-contractors' use of IT and management of data, the security risks faced by sub-contractors impact upon the organisations that engage them.

Risk importation occurs even in the case of conventional employees, because of the Bring Your Own Device (BYOD) phenomenon. On the one hand, this outsources IT device provision from the employer to the employee. On the other, it insources to the employer the insecurities of their employees' devices. A key risk is that data on which the organisation depends may not be subject to adequate backup and recovery arrangements.

A prior study was undertaken of the risks involved in consumer migration from local applications to remote services (Clarke, 2011). That paper concluded with the following quotation: "Some cloud computing outfit is going to quickly and quietly shut down, taking with it the data (business, photos, video, memories, etc.) of tens of thousands of users. Once we're storing everything in the cloud, what's to keep us from *losing* everything in the cloud?" (Cringely, 2011, emphasis in original). Clarke (2012) documented the extent and nature of cloud interruptions and failures in the period 2005-11. The present paper is motivated by the need for clear guidance for small users faced with such service-provider frailties.

1.2. *Backup and recovery*

A key purpose of backup and recovery arrangements is to ensure that data continues to be available in its appropriate form, despite loss of, or compromise to, the primary copy. A range of alternative approaches exists. References of value to the research reported here were Chervenak et al. (1998), plus Lennon (2001), Gallagher (2002), Preston (2007), de Guise (2008), Strom (2010), TOB (2012) and Cole (2013).

Backup may be performed at the level of a database or a file. Alternatively, multiple versions of, or all changes to, data may be stored within a database or file. The separate copy/ies may be on the same storage-device, or on another local storage-device, or on a device in a known location that is sufficiently remote that it is not subject to the same local-area risks as the original copy, or on a device whose location is unknown. The copy/ies may be online or offline. The device(s) containing the copy/ies may be in the possession of the relevant entity or of another party. The relevant entity may or may not own the device(s) in question, and in either case, exercise by the entity of its rights may be subject to limitations because of the rights of other parties.

Backup processes vary in terms of their immediacy and frequency, their scale, the quality assurance applied to the resulting copy/ies, and their accessibility by the relevant entity, and by other authorised parties. A substantial range of alternative forms of backup procedures exists, including within-file backup that sustains version history, full and incremental backups of storage volumes, mirroring, and spooling to new media.

A predecessor paper reported on an in-depth analysis of the backup needs of micro-organisations and prosumers that store the primary copy of their data in-house, under their own responsibility (Clarke, 2016). That paper also addressed circumstances in which an entity uses a remote file-hosting service, but processes the files on the entity's devices. Appendix 2 to the predecessor paper provides comprehensive catalogues of the characteristics of backup data (incl. logical, physical and organisational locations, and accessibility), and of backup processes (incl. timeframe, scale, quality assurance and archival). Appendix 3 further identifies the contexts, processes and attributes of a dozen specific forms of backup procedure.

1.3. *The cloud*

During the last decade, the user's proximity to their data has diminished. The data used to be 'here', on the consumer's own device. It moved to 'there', as consumers used relatively local Internet Services Providers, with a known footprint. As the dependency came to be on large national ISPs, and particularly on ISPs outside the consumer's local jurisdiction, the footprint became less visible, and the data moved 'somewhere'. To the extent that cloud computing is applied, consumers' data is now 'anywhere'.

At the applications level, cloud computing takes the form of so-called [Application] Software as a Service (SaaS) offerings. Under the SaaS model, the service-provider both stores the primary copy of the data and performs much of the processing (Armbrust et al., 2010; Höfer and Karagiannis, 2011). The user has a relatively thin application on their desktop and/or laptop, in many cases in the form of scripts downloaded to their browsers, or a small 'app' on their smartphone and/or tablet.

The term 'SaaS' is often associated with office automation services such as Google Docs, and the customer relationship management (CRM) service Salesforce. However, the pattern was emergent for some years, in such forms as webmail (operated both by local ISPs and by large providers such as Hotmail, Yahoo! and Gmail), family-tree data (e.g. ancestry.com) and textual documents, commonly called web-logs or blogs (e.g. wordpress.com). The more sophisticated forms that have emerged since about 2005 extend 'outsourcing' to 'cloudsourcing' by taking advantage of inexpensive commoditised hosts and virtualisation features, which has had the effect of articulating the industry into a wholesale-retail network model.

A SaaS segmentation analysis was presented in Clarke (2011). Since then, however, there have been further developments in SaaS offerings. No empirically based taxonomy was located in the formal literature. One reason for this is that market offerings continue to develop. For example, backup as a service, and disaster recovery as a service, were emergent during the period during which this study was undertaken. The following segments are proposed as a means of identifying potential objects of study, based on examples and partial classification schemes evident in both refereed and commercial literatures:

- **Communications and Collaboration Services**
  Examples include email services such as Yahoo!, Hotmail and Gmail, proprietary asynchronous messaging services, synchronous messaging services (chat, Instant Messaging), shared diaries, and project management services:

Please cite this article in press as: Roger Clarke, Can small users recover from the cloud?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.08.004