ephemera
theory & politics in organization

ISSN 1473-2866 (Online)
www.ephemerajournal.org
volume 21(1)

Standing by for data loss: Failure, preparedness and the cloud

A.R.E. Taylor

abstract

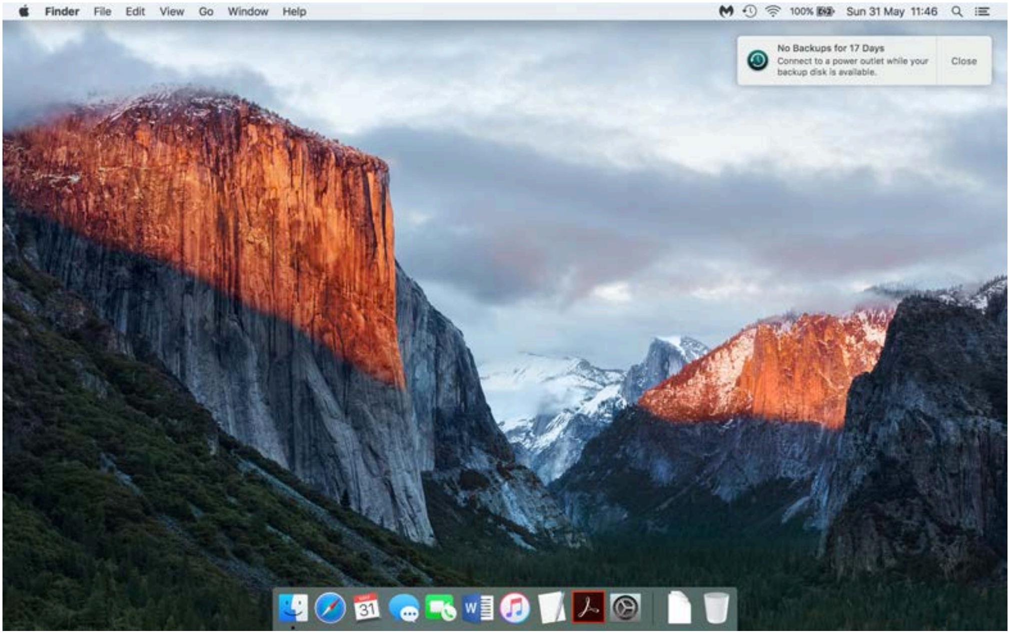
This article explores how the anticipated failure of digital technologies positions cloud storage providers and cloud users on 'standby' for data loss. With their fragile components and limited lifespans, digital devices are not built to last. Users must take preparatory action if they want to avoid losing data when their devices fail. Cloud-based back-up solutions have emerged as key technologies with which individuals and organisations prepare for data loss. For a monthly subscription, cloud providers offer an online data storage space safely removed from the local storage of personal devices or office computer systems, with the promise that clients' data will be protected and continuously available. Yet for those who work in the data centres that underpin the cloud, ensuring this constant availability requires a tremendous amount of equipment, infrastructure and human labour. With reputational damage and revenue at stake with every second of data centre downtime, 'standby' arises as the guiding logic for organising the operations of cloud infrastructure and the daily working lives of those who manage and maintain it. Drawing from ethnographic fieldwork, this article traces the technologies, affects and 'backed up' subjects that standing by for data loss generates in and out of the cloud, and embeds cloud storage within a longstanding industry of data back-up, recovery and salvage services. The prospect of data loss, it is argued, arises as both a growing threat and opportunity in digital capitalism, as the accelerating obsolescence of our digital technologies increasingly makes data 'preppers' of us all.

Introduction

> Okay. Now everything on your other phone and on your hard drive is accessible here on the tablet and your new phone, but it's also backed up in the cloud and in our servers. Your music, your photos, your messages, your data. It can never be lost. You lose this tablet or phone, it takes exactly six minutes to retrieve all your stuff and dump it on the next one. It'll be here next year and next century. (Brandon, in Dave Eggers' *The Circle*, 2013: 43)

I begin with this short excerpt from Dave Eggers' 2013 techno-dystopian novel *The Circle* because it captures the promise of transcendental and perpetual data storage that lies at the heart of cloud computing. If digital technologies are prone to failure, the cloud purports to provide users, be they individuals or organisations, with a space in which they can safely store their data beyond the fragile material forms of their personal devices or office IT systems. Cloud providers strive to ensure that no matter what should happen to users' smartphones, tablets or computers, the data from these devices, backed-up in their data centres, is continuously available, ready to be instantly retrieved and re-downloaded without delay.

This article explores how the anticipated failure of digital technologies positions cloud storage providers and cloud users on 'standby' for data loss. 'Standing by for data loss' describes an affective mode of living towards an anticipated future of technology failure and taking preparatory measures in the present to ensure that device breakdown doesn't result in data loss. Packed full of fragile microelectronics and with their ever-shortening lifespans, the digital devices that surround us are often not built to last. Consumers are increasingly aware that failure is strategically built into these electronics. Planned obsolescence, battery degradation and black-boxed, unrepairable devices sustain a culture of perpetual upgrading, leading to ever-accumulating (and unevenly distributed) deposits of e-waste (Parks, 2007; LeBel, 2012). The regularity with which digital technologies crash, malfunction or otherwise fail, increasingly requires their users to stand by for their inevitable decline and take anticipatory action if they want to avoid losing the valuable files stored on their devices. Programs like Apple's 'Time Machine' or Windows' 'Backup and Restore' make it easy for users to back-up their computers onto external hard drives. These programs regularly prompt users with push notifications if a back-up is overdue, reminding them that device failure and data loss can occur at any moment, for which they must be prepared (Figure 1). Increasingly, more and more users are turning to cloud storage solutions to back-up their files online. Dropbox, Google Drive, Apple's iCloud, Microsoft's OneDrive and other cloud services provide users with quick, easy and supposedly infinite data storage space, for a monthly subscription fee.



No Backups for 17 Days
Connect to a power outlet while your backup disk is available.

Figure 1: A push notification from Apple's Time Machine application in the top right corner of the screen reminds the user to back-up their computer. Screenshot by A.R.E. Taylor.

Backing-up into the cloud has the advantage of requiring little action on the user's part. If backing-up to an external hard drive is a task that users easily postpone, most cloud services offer to automatically back-up device data at a designated time of day (providing there is a Wi-Fi connection). Most crucially, the cloud provides a centralised online data storage space from which users can access and synchronise their files across their devices. In doing so, cloud providers strive to render device breakdowns, thefts and upgrades as non-disruptive as possible by guaranteeing that user data will not be lost and is ready and waiting to be swiftly accessed and re-installed (within 'six minutes' in *The Circle*) on their next device as and when failure should arise. Yet, for those who work in the data centres where cloud data is stored, ensuring the constant availability of online data services is no easy task. Despite the image of transcendental data storage that the 'cloud' metaphor conjures, for data centre professionals, this infrastructure is experienced as material, highly fragile and prone to failure. IT failure is an inherent part of everyday working life in the cloud: computers crash, servers go down, connections time out and hard disk drives malfunction. To maintain the cloud's promise of uninterruptible, even eternal data storage (data that will, in Circle employee Brandon's words, 'be here next year and next century') requires a tremendous amount of infrastructure, energy and human labour. At the same time, as commercial cloud providers compete to attract business, they promise to guarantee increasingly extreme levels of data availability and system uptime that their competitors cannot match. Data centre uptime is measured by the number of 'nines' of critical system availability that a provider guarantees, typically ranging from services that will remain online for 90% of the time ('one nine') up to 99.99% of the time ('four nines'). In their service level agreements (SLAs), some data centre providers will even promise their clients up to 99.9999% service availability (which translates into only 31.56 seconds of downtime a year). Data centre professionals must thus navigate the requirement of needing to offer continuous service availability in the face of IT failure that is understood as inevitable. This calls forth 'standby' as the strategic operating logic of the data centre industry. Inside any data centre one encounters an array of back-up servers, generators, air conditioners and other equipment, idling in a state of readiness, waiting to be activated in the event of an emergency. Scaled up to the level of architecture, the logic of standby produces an ever-expanding network of data centres that are being constructed as back-up sites. Standby further arises as a more-than-material security practice, generating anticipative affects among data centre employees, who work on high alert, constantly attuned to the possibility of IT failure. It is, after all, their job that is on the line if they should be responsible for losing a client's data.[1]

[1] As Vincent Mosco (2014: 133) puts it, 'engineers working for cloud companies labor in fear of losing their jobs if they are caught with their servers down'.

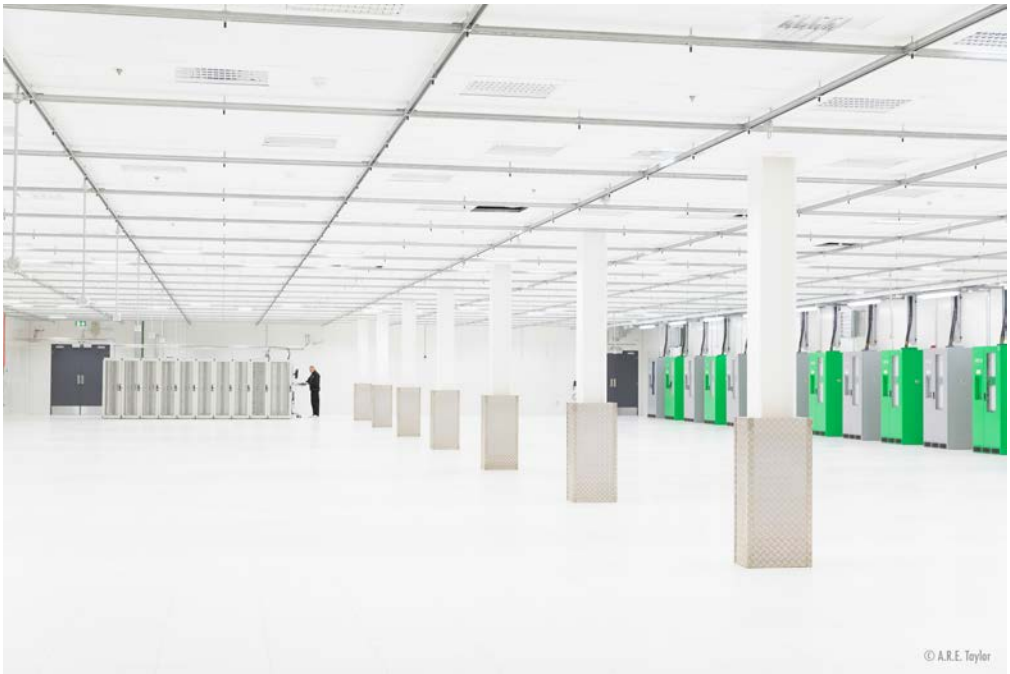


Figure 2: A technician runs diagnostic tests as part of routine server maintenance in a London data centre. Photo by A.R.E. Taylor.

Standing by for data loss, for cloud users and cloud providers alike, thus entails occupying a specific subject position in relation to the precarious nature of digital technologies. This mode of standby materialises in the form of back-up hard drives or cloud subscriptions at the user-end, and redundant servers, power generators and back-up data centres at the service-provider end.

A focus on the subjectivities and practices that standing by for data loss generates, provides an entry-point for thinking about the convergence of digital capitalism and disaster capitalism. Naomi Klein (2007) has used the phrase 'disaster capitalism' to describe the political-economic complex that converts disasters into profitable opportunities under neoliberal rule. Klein is predominantly concerned with the exceptional policy or economic measures (often involving deregulation schemes and the promotion of privatisation) that neoliberal reformers justify in the wake of disaster events. Media scholar Wendy Chun (2016) has taken some steps towards embedding digital media technologies within the context of catastrophe-orientated capitalism. Chun productively links practices of device updating to the perpetual state of crisis that has been widely theorised as forming the operating conditions of neoliberal economics. Chun's work provides an entry-point for exploring how the rapid obsolescence, regular breakdowns and other 'crises' that shape user experiences of digital media technologies, encourage habits of constant upgrading. 'In new media, crisis has found its medium', Chun (2016: 74) writes, 'and in crisis, new media has found its value'. Commenting on the economic value of failure-ridden digital devices, Arjun Appadurai and Neta Alexander (2020: 23) have observed that '[t]echnological failures such as limited battery life, digital lags, or frozen, irresponsive screens effectively support a business model of upgrading'. But device failure is not only rendered economically productive through consumers perpetually upgrading or replacing their digital gadgets. Just as disasters do not need to occur in order to be rendered profitable (as we see with private sector consultancies that make money from selling preparedness services), device failure and the ensuing crisis of data loss does not need to materialise in order to generate economic value. Indeed, the cloud enables technology corporations to extract profit from the mere prospect of device failure, by encouraging users to invest in data back-up and recovery services to ensure that IT malfunction does not result in data loss. If, as Paul Virilio (2007) famously suggested, new technologies produce new opportunities for technological failure, in doing so, they also open up new markets for the *anticipation* of failure.

The cloud itself is merely the latest instantiation of a longstanding industry of data back-up and IT disaster recovery services that has steadily emerged since the mid-late twentieth century precisely to capitalise on the anticipated prospect of data loss, as precarious computer systems became permanent fixtures in organisational environments. The aim of this article is thus to draw attention to the cloud data centre not simply as a built response to growing demands for data storage (i.e. an architectural solution to the so-called 'data deluge') but as part of an ever-expanding economy of 'data preparedness' that has arisen since the late 1960s to protect against - and profit from - the unending prospect of data loss that lurks in the background of daily life in an increasingly digital world.

The material presented here is based on empirical data collected from ongoing fieldwork that I have been conducting in the data centre industry since summer 2015 (Taylor, 2019; 2021). During this time, I have shadowed the work of data centre professionals, including data centre managers, security guards, disaster recovery consultants and IT technicians, as well as attended data centre industry events and training programmes. The historical material in this article draws from archival IT industry magazines as well as interviews with data centre professionals, many of whom have worked in the industry for the last forty years. The discussion that follows is predominantly situated at the intersection of two literatures. The first is the body of scholarly work on preparedness which has explored how this anticipatory security rationality has emerged as a key strategic logic through which everyday life has come to be organised (Lakoff, 2006: 265, 2017; Anderson, 2010). The second body of literature is the recent work in media, technology and infrastructure studies, that has turned to breakdown, malfunction, repair and failure as theoretical and methodological frameworks for studying the materialities of digital technologies as well their supporting infrastructures, industries and workers (or 'maintainers') (Graham and Thrift, 2007; Jackson, 2014; Carroll, 2017; Russell and Vinsel, 2018; 2020; Mattern, 2018; Graziano and Trogal, 2019; Appadurai and Alexander, 2020).

Amidst growing interest in media materialities, the broken computers, frozen loading screens and outdated phones that we frequently encounter today have provided windows onto the limitations of technological progress and the narratives of newness and innovation that underpin their development, design and marketing (Gabrys, 2013; Alexander, 2017; Russell and Vinsel, 2018; 2020). Discarded digital objects have also surfaced as valuable entry-points for exploring contemporary configurations of capitalism, particularly the unethical and unsustainable operating logics of a technology industry that capitalises on the failure of digital commodities (Mantz, 2008; Burrell, 2012). While discarded devices are now drawing significant scholarly attention, a focus on the cloud as a technology of preparedness expands the temporal horizons of existing studies of failed digital technologies, directing attention to the anticipation rather than aftermath of failure. Indeed, if failure has become an inevitable, or even accepted future of digital devices for consumers, this is partly because an entire infrastructure of data preparedness has arisen to render device failure as non-disruptive and tolerable as possible by ensuring that the data contained on these technologies is not lost along with them. The cloud is a key service through which the anticipated disaster of device failure is transformed from a shocking or rupturing event into a forgettable, permissible and (relatively) non-disruptive event. By striving to ensure that device failure does not result in data loss and by ensuring that data can be quickly re-downloaded onto a new device, the cloud, I ultimately argue, both capitalises on the prospect of data loss and also facilitates the quick and easy turnover of digital electronics, bolstering a techno-economic system based on planned obsolescence and perpetual upgrades.

This first two sections of this article trace the role that cloud back-up and recovery services play in end-user plans for anticipating IT failure. I begin by sketching an analysis of the basic logic of data preparedness that underpins and drives practices of standing by for data loss. I then trace a brief history of data preparedness from an IT disaster recovery perspective, exploring the role that data back-up vendors and, later, cloud providers have played in this security market. The final two sections of this article move us into the 'cloud' to look at the work that standing by for data loss entails in the data centre industry, focusing on the hypervigilant data centre subjectivities as well as the material infrastructure and equipment through which standby is measured and produced in the cloud.

Data preparedness

Originally sponsored by cloud back-up vendors such as Crashplan and Backblaze, since 2011, March 31 has been designated 'World Back-up Day' (Figure 3). An introductory video on the official World Back-up Day website invites visitors to imagine various data loss scenarios, such as their smartphones being stolen or their computers crashing, asking, 'What would you do if you lost everything?' and 'What would you lose forever?' Encouraging viewers to imagine their data under threat and to accordingly develop the habit of backing-up their devices regularly, these rhetorical prompts aim to transform users into responsible 'backed-up' subjects. Here, the present is configured as a time-space of impending device failure in which users must take appropriate anticipatory action to protect the photos, files and other precious data stored on their personal electronics. Technological failure is positioned as something that cannot be prevented. Computers will inevitably crash and smartphones will inevitably be stolen, lost or irreparably damaged, but, with the right preparations, by internalising a rationality of preparedness, users can ensure that they don't lose their data along with their devices.

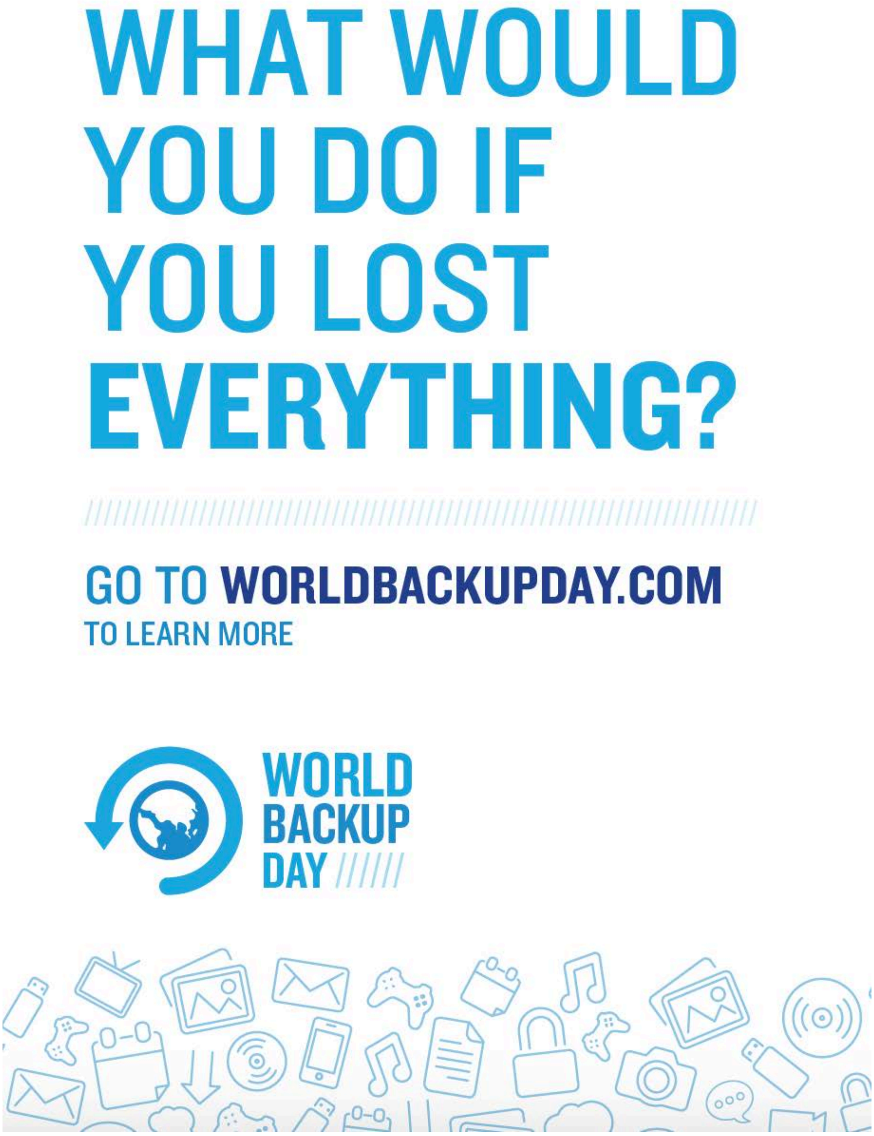


Figure 3: A promotional poster for the annual awareness day ‘World Back-up Day’. A video on the World Back-up Day website informs visitors that: ‘More than sixty-million computers will fail worldwide this year. And that's not all. More than two-hundred-thousand smartphones are lost or stolen every year. That's countless irreplaceable documents and treasured memories destroyed’. Image from worldbackupday.com, reproduced under Fair Use Licence.

'Preparedness' has been loosely defined by anthropologist Frédéric Keck (2016) as 'a state of vigilance cultivated through the imagination of disaster'. By envisioning dystopian future scenarios, preparedness practitioners seek to produce and administer a world in which threatening events do not catch humanity off guard. These threatening events - which can range from pandemic outbreaks to cyberattacks to extreme weather events – are constructed as inevitable and unpreventable, but potentially manageable if the right measures are taken to anticipate them. If action is not taken, 'a threshold will be crossed and a disastrous future will come about' (Anderson, 2010: 780). Preparedness emerged as part of Cold War civil defence projects to secure the future when faced with the need to anticipate a surprise nuclear attack (Collier and Lakoff, 2010; 2015). The probability and predictability of such an attack was not calculable and the potentially catastrophic consequences were equally incalculable. Preparedness thus surfaced as a style of reasoning with which security planners and strategists could grapple with 'a foreseeable, but not statistically calculable event' (Lakoff, 2008: 406). Rather than rely on risk-based statistical and calculative methods for managing uncertainty, under the rubric of preparedness Cold War strategists developed imaginative new methods such as duck-and-cover drills, scenario planning, disaster simulations and resource stockpiling, as tools with which they could prepare the nation for thermonuclear warfare. Through these techniques, new modes of civilian and military subjectivity were generated that could live with the constant possibility of annihilation (Lutz, 1997).

While preparedness was most fully articulated as a mode of governance during the Cold War, throughout the second half of the twentieth century, practices of preparedness were mobilised as generic tools with which to manage a diversity of disaster scenarios across a range of sectors and policy domains, from public health to international terrorism to critical infrastructure protection (Lakoff, 2008; Collier and Lakoff, 2015). In the process, new security markets for preparedness have emerged, with private sector consultancies providing 'business continuity' advice, guidance and resources. Preparedness does not only offer a formal framework for governments and organisations to manage uncertainty. As the permanent crises and intensifying conditions of everyday insecurity associated with late neoliberalism accelerate, preparedness has also increasingly seeped into everyday life, giving rise to growing communities of ‘preppers’ (Huddleston, 2017; Mills, 2018; Garrett, 2020). By conjuring the perpetual potential for disaster, preparedness fosters subjects that can adapt themselves to ever-expanding horizons of threat and precarity, often under the imperative of becoming ‘resilient’ (Grove, 2016: 30; Chandler and Reid, 2014).

If conditions of perpetual threat entail the production of new forms of preparedness among populations, then the ever-present possibility of digital device failure has made standing by for data loss part of the fabric of everyday life in the digital world. Standing by for data loss arises as a normative affective state when the prospect of digital device or IT system failure becomes an imminent and permanent possibility, requiring digital citizens to partake in routinised practices of backing-up their data. A ‘how-to’ guide on cloud back-ups articulates the basic logic of data preparedness: ‘If something untoward should happen to your computer, then a good backup is all that stands between you and complete disaster - it may seem like a chore to duplicate all your files but you’re going to be glad you did if your machine gets beyond repair’ (Nield, 2015). Backing up, it is hoped, can prevent device failure from escalating into the disaster of data loss.

While devices are largely replaceable, the data they contain is not. Losing the digital photos, videos and other files that users store on their smartphones, tablets, laptops and personal devices could be a potentially devastating experience. Natasha Dow Schüll (2018: 44) has used the language of existential risk to capture the impact of data loss on peoples’ lives today, describing ‘the annihilating sense of loss that strikes when personal information archives crash, inexplicably disappear into the ether of the so-called cloud, or become mysteriously corrupt and inextractable’.[2] For most organisations today, data loss has a similarly existential quality to it, potentially putting an end to their operations. Data loss has gradually surfaced as a growing fixture in the collective imagination of catastrophic futures in recent decades. The plots of films like *Blade Runner 2049* (2017), TV shows like *Mr Robot* (2015-2019) and graphic novels like Enki Bilal’s *Bug* (2017) all pivot around large-scale data erasure events that lead to widespread

[2] Shannon Mattern (2018) has similarly observed that, for the techno-dependent citizens of the global north, ‘a cracked screen can mean death’.

societal collapse.[3] In other equally dystopian visions, with more and more cultural heritage now being 'born' digital or rapidly being digitised as part of preservation programmes, a growing number of digital archiving projects have been motivated by the prospect of the 'digital dark age'; a future scenario in which vast swathes of data are lost due to obsolescence, digital decay or bit rot.

While imaginaries of data-based disasters are intensifying, data loss has long been a source of threat for businesses and organisations constructed around a dependence on digital computer systems and the data they generate.[4] In the following section, I explore how the prospect of data loss has energised an entire industry dedicated to data preparedness since the late 1960s. A longstanding body of scholarship has examined the critical role that information technologies play within modern capitalist economies (Beniger, 1986; Castells, 1996; Zuboff, 1988; Mahoney. 1988; Rochlin, 1997), as well as the new horizons of threat, such as cyberattacks and computer bugs, that IT systems enabled (Cavelty, 2008; Edwards, 1998; McKinney and Mulvin, 2019). Less attention, however, has been directed towards the data back-up and recovery industry that developed in tandem with the integration of digital computing systems into everyday life, as well as the threat (and opportunity) that data loss has long posed to digital capitalism.

[3] *Blade Runner 2049* is set in the aftermath of a mass data loss event known as 'The Blackout' in which electronic records have been wiped. This event is dramatised in the official online prequel *Blackout 2022* (2017). *Mr Robot* focuses on a hacker who erases the consumer debt records held by a multinational conglomerate. *Bug* is set in 2041 where a computer virus manufactured by extra-terrestrials wipes data from every digital device in the world, depriving citizens of their 'digital addiction'.

[4] The history of protecting non-digital data extends far beyond the practices described here and would include data storage sites such as libraries, museums and archives. In some cases, digital data storage sites have been located in the same material spaces that were originally used as document vaults for the storage of valuable paper records, such as bank documents or sensitive medical and legal files, e.g. see Tung-Hui Hu's (2015: 96-97) discussion of the data management company Iron Mountain.

Standing by for data loss: A brief history

With the introduction of general-purpose business computers, such as the IBM 360 (1965) and IBM 370 (1970), into organisational environments, the loss of vital digital records was increasingly understood as a threat of potentially disastrous proportions, for which anticipatory measures needed to be taken. Large bureaucracies, such as governments and multidivisional corporations, quickly became dependent on their computer systems. Yet digital computers were susceptible to failure and their rapid and widespread use opened up new fronts of data-based vulnerability. As disaster preparedness and crisis management became norms of organisational practice in the 1960s and 1970s (Hermann, 1963), organisations turned their attention towards their electronic data processing (EDP) activities (Herbane, 2010: 982). This led to the development and implementation of new forms of business continuity management, such as IT disaster recovery, that sought to integrate the protection of precarious computer systems into crisis planning.

The prospect of data loss presented new opportunities for profit. A commercial IT disaster recovery industry swiftly emerged, comprising of data back-up, restoration and salvage services as well as suppliers of emergency recovery centres. Sun Information Systems (which later became Sungard Availability Services) became one of the first major commercial disaster recovery vendors, established in 1978 in Philadelphia. Cisco Systems, founded in 1984, quickly followed. Disaster recovery vendors offered subscriptions to dedicated recovery sites and back-up services, providing standby IT resources with the aim of ensuring that the failure of an organisation's computer system would not result in significant or disruptive data loss. These vendors would copy critical data onto a direct access storage device (DASD) (magnetic tape was the most frequently used digital storage media until the early 2000s). This data back-up work was typically undertaken by storage managers working overnight on 'graveyard' shifts when the organisation's operations were not running. After the system data was copied to tape, it would be stored at a secure off-site facility. Should a disaster arise, these vendors would deliver the tape to the client's workplace, mount it on their computer systems and then re-load it so the organisation could begin operations, usually within twenty-four hours.[5] As well as providing off-site data storage, disaster recovery contractors also provided emergency recovery sites that often came in three forms: hot, warm and cold.[6] The metaphor of temperature was used to describe different temporalities (and price points) of recovery in relation to different modes of standby IT infrastructure: hot sites duplicated an organisation's entire infrastructure at an alternative location so they could simply transfer staff to this site and continue operations almost immediately; warm sites allowed some, but not all of the core processes to be resumed immediately; cold sites simply provided an alternative site to set up operations in the event of a disaster striking the day-to-day workplace.

As 'always-on' computing became a standard business requirement over the next two decades, any duration of downtime became increasingly unfeasible. Loss of access to data, even for short lengths of time, could be disastrous for data-dependent businesses, both financially and legally. In the late 1980s, two out of every five companies that experienced a major data loss disaster never resumed operations (Radding, 1999: 8). The sheer volume of data that organisations were now working with, and the pressure to back-up and restore data fast, led to the development of new storage techniques and technologies. The increasing availability of high-speed, low-cost fibre connections in urban centres of the global north meant that clients could now back-up and retrieve their data remotely. This model of remote back-up formed the foundation for cloud-based back-up and recovery.

Cloud computing enables clients to access files over a network as if they are stored locally on their computer systems. At its most basic, the cloud marks a shift in data storage practices from storing information locally on the hard drives of personal computers to a form of online data storage, where files are

[5] The history of IT disaster recovery is also a history of digital storage media. Magnetic tape became the storage medium of choice in the 1970s, replacing the punch card that had been the primary storage medium for mass-information processing since the late nineteenth century (Driscoll, 2012). In the 1990s, data storage managers would also use CDs and diskettes to back-up certain parts of a system, while hard disk drives became an affordable alternative for industrial-scale data storage operations in the late 1990s (Radding, 1999).

[6] As Wolfgang Ernst (2019: 42) has observed, '[t]he vocabulary of storage media is significantly dominated by the language of temperature'.

stored on the hard drives of servers in data centres that are accessed remotely 'as a service' through the Internet (Figure 4). For this reason, data centres are often described as sites where 'the cloud touches the ground' (Holt and Vonderau, 2015: 75; see also Bratton 2015: 111). Data centres had emerged in the late 1980s, when corporations began to share computing infrastructure in order to avoid the large capital outlays of purchasing expensive mainframe computers. However it was during the dot-com boom that the data centre became the dominant service model for corporate IT operations. The growing adoption of Internet technologies had made it cheaper, easier and quicker for firms to store and process data at a distance. Terrorist attacks in major urban centres in the early 1990s had also led to a growing corporate awareness of the need to move computing equipment out from their urban office complexes in order to further increase their chances of maintaining continuity during catastrophic events.[7] Offering greater physical security than office-based IT departments and round-the-clock maintenance, data centre providers promised their clients new forms of 'uninterruptible' reliability in the face of an ever-expanding horizon of security threats. Often including back-up and disaster recovery services as part of their packages, the aim of the data centre was not only to ensure that business-critical IT systems could 'recover' quickly in the event of failure, but to reduce the need to recover in the first place by investing in deployments of standby equipment and infrastructure.

[7] Such as the London Stock Exchange in 1990, the London financial district in 1992 and 1993, the World Trade Centre in 1993 and the Oklahoma City bombing in 1995. Terrorism would continue to drive demand for remote data storage. Observing the post-9/11 boom in data recovery services, urban theorist Mike Davis (2002: 12) commented that '[t]error, in effect, has become the business partner of technology providers'.

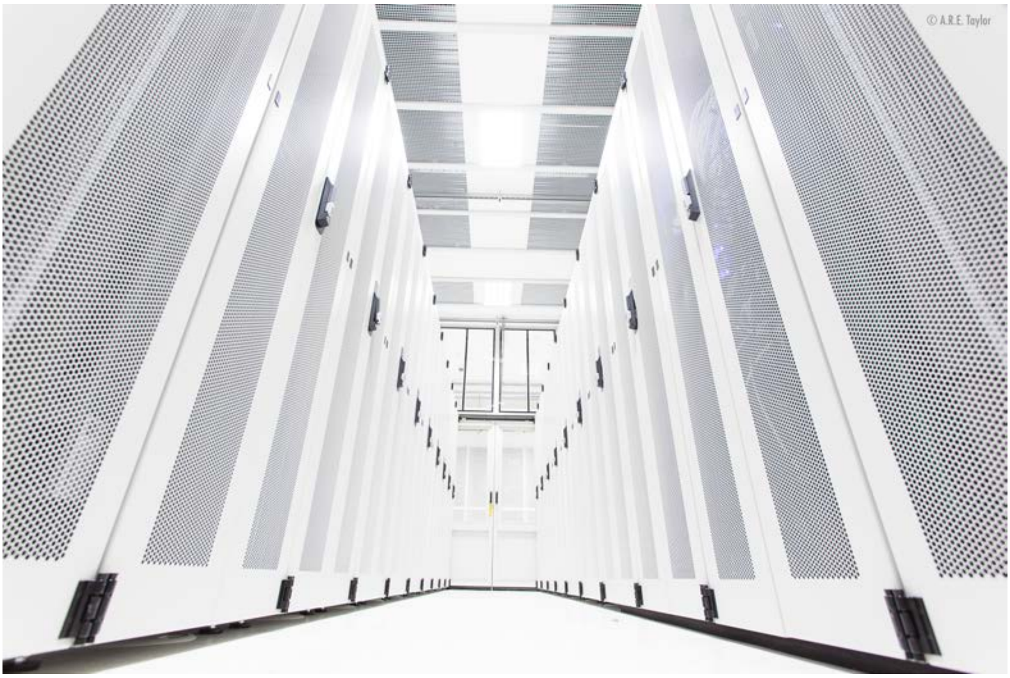


Figure 4: Cloud data is stored on the hard drives of servers (pizza-box shaped computing machines), which are securely encaged inside cabinets arranged in aisles. Photo by A.R.E. Taylor.

As microcomputers and portable digital gadgets began to disperse throughout the social field in the 1990s, standing by for data loss become an imperative not only for organisations but for individual end-users. New mass markets for data preparedness had already emerged a decade prior, with floppy disks providing back-up storage capacity. With users generating increasing volumes of digital information, data storage corporations like Western Digital and Seagate Technology began to manufacture portable back-up hard disk drive products for personal consumers. These had a greater storage capacity than media such as floppy disks and CDs. Of course, they were also prone to failure. If dropped, the data could become corrupted and, if not regularly used, their mechanical parts would deteriorate. From the mid-2000s, cloud storage providers began to target this new market of personal consumers, providing them with access to scalable online data storage in dedicated data centres that had previously only been available for industrial-scale storage operations.[8] If floppy disks and external hard drives were once primary technologies of personal data preparedness, the last decade has seen the cloud quickly taking on this role. For cloud users, with their data stowed away and automatically backed up in data centres, the anticipated disaster fades into the background operations of daily life: a constant possibility that they are nevertheless prepared for. This logic is nicely captured by the cloud back-up guide previously cited: 'backing up is now easier than ever: the new wave of cloud storage services can do the job for you in the background while you work' (Nield, 2015). However, the language of ease, simplicity and automation that underpins cloud back-up rhetoric erases the work that takes place behind the screens to deliver these services.

Standing by in the cloud

For those who work in the cloud, standing by for data loss surfaces as a state of anticipation for IT failure that could occur at any moment. Just as personal digital devices regularly crash, freeze or break down for consumers, so too, do the industrial servers and other computing equipment that fill the floorspace of data centres. While the cloud promises to protect data by separating it from the fragile materiality of personal devices and office computers, it does so by duplicating it on equally fragile servers in data centres that must be constantly maintained by technicians and storage managers. The inevitability of IT failure is captured by the preparedness maxims that are regularly repeated in data centre management training programmes and during talks at cloud security trade shows. When it comes to IT failure, 'it's only a matter of time', 'it's not a question of if, but when' and 'never say never' are phrases one frequently encounters in the industry. Such phrases seek to reduce complacency among data centre professionals, cultivating a sense of alertness for impending infrastructure failure for which they must perpetually prepare.

[8] The online back-up service Mozy was founded in 2005, while Dropbox was founded in 2007. That same year Microsoft launched OneDrive. In 2011, Apple launched iCloud and Google Drive was released in 2012.

Infrastructure studies and maintenance studies scholars have demonstrated that error, neglect, breakage and failure are not atypical of technological systems but 'a normal condition of their existence' (Graham and Thrift, 2007: 5; see also Henke, 1999; Star, 1999; Denis and Pontille, 2014; Russell and Vinsel, 2018; 2020).[9] If the idea of the 'cloud' may evoke imaginaries of weightless and placeless ethereality for those at the user-end, for the technicians and maintenance teams that work in the cloud this is certainly not the case.[10] The data centre professionals I met during my fieldwork often voiced concerns that the cloud's promise of transcendence beyond the material world leads to intense pressure to meet stringent service level agreements for data availability.[11] As one data hall technician told me, 'for most end-users, the cloud is the solution to their data loss problems [but] what most of them don't realise is that the problem hasn't disappeared, it's just become someone else's problem, our problem'. Data centre professionals primarily address this 'problem' through the deployment of standby resources. Standby capability and capacity, in the form of redundant or back-up systems and reserve staff, has long played a central role in building preparedness in organisational contexts where very high levels of operational reliability must be maintained. Much like nuclear power plants, aircraft

[9] Ethnographic work has demonstrated that perceptions that infrastructures remain 'hidden' or 'invisible' until breakdown are unable to adequately capture the 'range of visibilities' (Larkin, 2013: 336) that shape different social groups' experiences of infrastructure services. As Shannon Mattern (2016) has observed, '[t]he presumption that infrastructures are "hidden" [...] signals great privilege.' The experience of infrastructure failure is thus unevenly distributed across social and geopolitical vectors. Malfunction is particularly visible for maintenance workers, whose work ensures that breakdown remains invisible for service end-users. The disruption of infrastructure and technology service provision is also a regular occurrence for those who live in the global south (Graham, 2010; Harvey and Knox, 2015; Trovalla and Trovalla, 2015). For discussions of the different registers through which cloud data centre visibility is governed, see Furlong (2020) and Taylor (2021).

[10] As David Ribes and Thomas A. Finholt (2009: 378) have observed 'one person's infrastructure is another person's daily routine of upkeep' (see also Star and Ruhleder, 1994).

[11] Elsewhere (Taylor, 2021) I have explored how the material vulnerability of cloud storage is leveraged in the marketing practices of commercial data centres that have been retrofitted inside nuclear bunkers.

control centres, power distribution grids and other high-reliability organisations, the standby imperative that underpins cloud infrastructure is similarly rooted in logics of 'excess, redundancy, and contingency, governed by the looming specter of worst-case scenarios' (Holt and Vonderau, 2015: 205).

Driven by the imperative of guaranteeing unstoppable operation in the face of a range of failure scenarios, data centres ensure that their critical systems are always backed up, with the aim of eradicating any single points of failure. The basic logic that guides this practice is that of 'N+1 redundancy': for every primary system or piece of equipment (N) there must be at least one duplicate (+1) to support the goal of uninterruptable service continuity and avoid unplanned disruption. There are a number of variations of this formula, such as N+2, 2N or 2N+1, each of which refer to different levels of data centre redundancy. Certification and standards organisations offer various tier systems that evaluate and classify data centre resilience, which is measured through performance history and the levels of back-up equipment and infrastructure a facility has available.[12] One of the most prominent international standards for evaluating data centre resilience was developed by the Uptime Institute, a US-based advisory and certification body established in the mid-1990s. The Uptime Institute uses a tier scale system that has been widely adopted throughout the data centre industry as a tool to rate and certify the maintenance, power, cooling and fault capabilities of a facility. A Tier I data centre will have basic redundant capacity in the form of chillers, pumps, engine generators and uninterruptible power supply (UPS) modules for power outages and spikes. At the other end of the scale, Tier IV data centres are 'fault tolerant facilities' that have multiple independent and physically isolated systems, as well as several independent active distribution paths to the compute devices. When equipment fails, or if there is an

[12] While the Uptime Institute is globally recognised, other data centre resilience standards are also used throughout the industry. The Telecommunications Industry Association's TIA-942-A Telecommunications Infrastructure Standard for Data Centers also users a tier model. Syska Hennessy use a classification system based on ten Criticality Levels. The UK-based Building Industry Consulting Service International (BICSI) categorises data centre availability into four classes: Class F1 (99.0% uptime); Class F2 (99.9% uptime); Class F3 (99.99% uptime); and Class F4 (99.999% uptime).

interruption in the distribution path, IT operations should not be affected. While the Tiers are progressive, this progression does not mean that a Tier IV facility is superior to a Tier I, II or III. Rather, these Tiers align with different business needs and requirements.

In the data centre industry, standby is both an energy-intensive and capital-intensive enterprise. Powering, cooling and maintaining data centre equipment is an expensive process. Servers consume considerable sums of electricity and generate huge amounts of heat (Velkova 2016). This requires extensive investments in air conditioning systems to prevent overheating, which adds to the electricity and water consumption costs (Hogan 2015). The extreme energy consumption of the data centre industry has been widely noted, with some reports suggesting that 'if the cloud were a country, it would have the fifth largest electricity demand in the world' (Greenpeace, 2012: 10). The duplication of equipment under the standby imperative thus further adds to the already significant capital outlay and carbon costs of the data centre. The logic of preparedness that drives data centre security discourses and practices leads many facilities to operate their power and cooling systems 'at excess capacities of upwards of 80 percent' (Furlong, 2020: 4), with the aim of anticipating any sudden spikes in demand. While in most cases a data centre will never reach the maximum loads it prepares for, this spare power and cooling capacity reassures data centre operators and their clients that their facilities are 'ready for anything'. The cost of standby is in fact often higher than that of running the facility. Based on an investigation into data centre energy use, *New York Times* journalist James Glanz (2012) reported that, on average, the data centres analysed used only 6-12% of their electricity to power their servers. 'The rest', Glanz observed, 'was essentially used to keep servers idling and ready in case of a surge in activity that could slow or crash their operations'.[13] New models of data centre capacity planning have arisen over the last decade with the aim of alleviating the operational expense (and carbon footprint) of overprovisioning. Yet, as data centre professionals strive to balance criticality against cost, excess capacity remains a relatively standard operating condition.

[13] Vincent Mosco (2014: 133) thus sums up the driving logic of standby in the data centre industry: 'Better to power unused servers than to face an angry customer'.

Data centres require multiple sources of power generation to deliver their uninterrupted service provision. Back-up power systems, often in the form of diesel-powered generators, are used when the primary electricity supply shuts down. For data centre professionals, every second counts during downtime and a big drawback of most diesel generators is that there is a 5-40 second period between mains failure and the generator coming online. While diesel generators are able to provide a longer-term power supply, valuable data could be lost in the few seconds they take to start up. This problem is typically overcome by using an uninterruptible power supply (UPS) system. These systems are powered by batteries or flywheels and are able to power most critical loads for a short amount of time (usually fifteen to twenty minutes) until the standby generator is ready. This UPS/generator combination enables data centre providers to promise their clients ‘total power protection’.

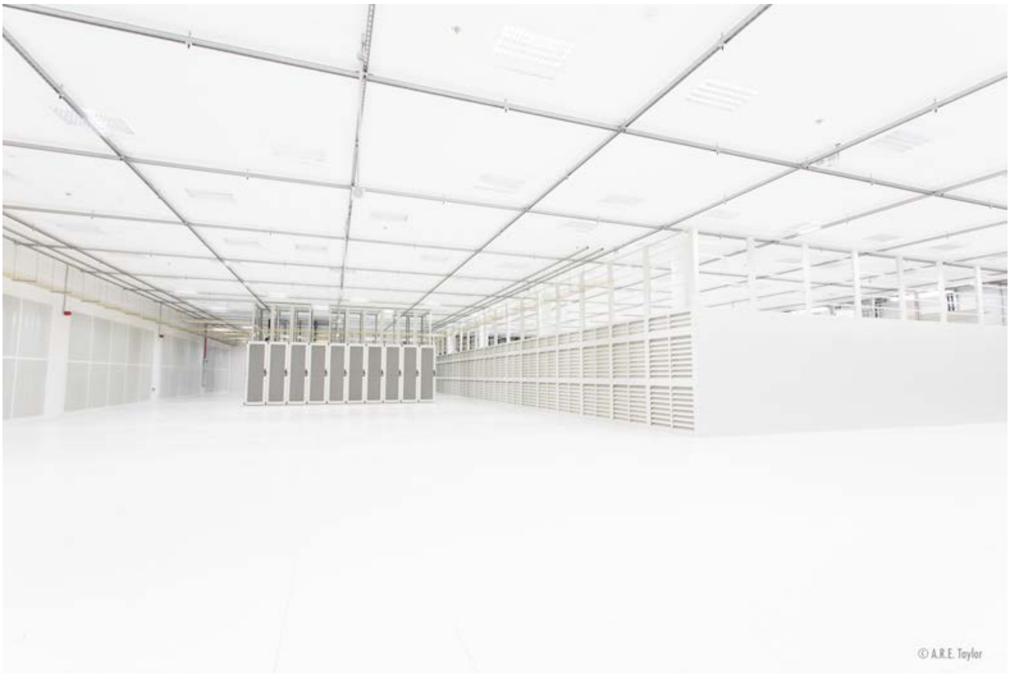


Figure 5: Servers wait on standby in a cloud provider’s back-up data centre. Photo by A.R.E. Taylor.

As well as investing in standby equipment within the facility, the standby imperative also spawns an ever-expanding range of back-up data centres that are often distributed across different geographic regions. Through the construction of multiple, globally-distributed facilities that operate as mirror images of each other, cloud providers strive to ensure that client data is constantly available. If for any reason the primary data centre should experience a local-level outage (due to fires, flooding, power loss, system failure, security breaches, etc.), it will automatically switch over, or, in data centre parlance, 'failover', to the back-up data centre(s), which is ideally located outside of the disaster region. This model of service delivery is known as an 'active-passive' deployment because the back-up data centre does not actively participate within the system during normal operation. Ever-increasing demands on data centre availability have led to new models of infrastructure provision that increasingly push beyond the logic of standby. For example, in 'active-active' setups, where multiple data centres jointly deliver an organisation's IT services simultaneously, there is no 'standby' data centre as such. Rather, all of a cloud provider's data centres are switched on and co-delivering services, blurring distinctions between 'primary' and 'standby' facilities. If one data centre should fail, then the others will pick up the workload, with the aim of ensuring that clients' files are always available and accessible. The end result of this extensive failover infrastructure is 'a massively-distributed geography of back-up and repair spread across the world' (Graham, 2015: 30). While standby equipment and infrastructure has a significant environmental and financial impact, data centre professionals justify this continuous investment with the argument that 'the cost of preparedness is much smaller than the cost of disaster'.

Significantly, standby equipment does not prevent failures from arising. Rather, it promises to reduce the impact of failure, with the aim of preventing unplanned errors or malfunctions (such as hardware failures or network errors) from escalating into catastrophic events. Vincent Mosco (2014: 130) has highlighted the Sisyphean nature of this investment in standby, reminding us that, 'even with all of this expensive, polluting backup, there is still no guarantee of 24/7 performance'. Mosco's observation parallels that of disaster recovery specialists. As any disaster recovery planning manual will highlight: 'no amount of preparation and backup systems can totally eliminate the risk posed by emergencies' (Gustin, 2010: 209). The aim of such guidance is to reduce complacency among preparedness practitioners, encouraging them to remain vigilant and alert, especially after standby equipment has been put in place, when temptations to relax might set in. To this end, data centre failure scenarios perpetually circulate in the data centre industry and play an important role in cultivating an affective state of readiness for disaster among data centre workforces.

During data centre training and security programmes, instructors provide course attendees with a seemingly never-ending list of threats to data centres. Along with the widely known risks of cyberattacks and human error, myriad other dangers pose a threat to the continuous operation of these buildings (McMillan, 2012). Subterranean and undersea fibre-optic cables are regularly cut by ships dropping anchor or by construction equipment at building sites (Starosielski, 2015). Particulate matter in the form of dust or pollen can block server fans, causing vital equipment to overheat. Weeds can cause damage to the foundations of data centres if left to grow, producing a potential point of structural vulnerability. Squirrels regularly chew through cable, causing damage to aerial fibre. Threats to data centre security thus extend across scales from the sub-visible worlds of particulate matter to malicious rodents and vegetation, to cyberterrorists, to the complacency or negligence of staff (Taylor and Velkova, 2021). Like any large infrastructure, the cloud is a fragile and unpredictable assemblage of people and things, with data centre failure often throwing into sharp relief complex entanglements of human and nonhuman activity (Bennett, 2005). As media scholar and former network engineer Tung-Hui Hu (2015: ix) has observed, for ‘a multi-billion-dollar industry that claims 99.999 percent reliability’, the cloud ‘breaks far more often than you’d think’.

Data centre failure scenarios like these arise in industry training programmes as moral tales about lax security practices and the limitless horizon of threats that face the data centre professional. As such, they are valuable tools with which data centre staff are transformed into vigilant infrastructure operators, always on alert for events that could arise from even the most unexpected of sources. These scenarios are often accompanied with startling statistics about the financial fallout of failure. During a data centre management training course that I audited in London in 2016, the instructor informed the group that, ‘Time is money. On average a data centre will experience twenty-four minutes of downtime a year, which can translate into thousands of pounds of lost revenue for the data centre [and] even more for the clients who rely on that data. This is unacceptable.’ A 2016 report on data centre downtime quantified the average cost of an unplanned data centre outage at US$9,000 per minute, with the most expensive unplanned outage costing over US$17,000 per minute (Ponemon Institute, 2016).

Given the financial and reputational damage that downtime can cause, key data centre personnel must also ensure that they are contactable twenty-four hours a day, three-hundred-and-sixty-five days a year, in case a failure event should arise. Many of the data centre professionals with whom I worked used mobile apps to remotely check the current service levels of their facility when not at the workplace. As most data centres have clients that are globally dispersed, this state of readiness is maintained around the clock. The data centre managers with whom I spoke were perpetually 'on call'. It is not uncommon for managers to receive emergency phone calls in the middle of the night that require them to drive to their workplace to tend to some unfolding scenario. It thus takes considerable work, energy and infrastructure to realise the cloud's promise of 'indefinite continuance' (Schüll, 2018: 45).

Failure, denied?

Standing by for data loss thus arises in the cloud both as an affective anticipatory state and as an infrastructural condition. Guided by the techno-economic imperative of ensuring uninterruptible data availability, standby is the default mode of organising the operations of digital-industrial infrastructure and the daily working lives of those who manage and maintain it. Standby equipment and multi-sited data delivery models aim to render data continuously available in the face of ever-present technological failure, with multiple facilities either co-delivering services or waiting on standby to immediately respond to disasters in real-time. While the failure of data centre equipment is frequently experienced (and imagined) by data centre staff, by choreographing and connecting an expanding network of data centres, cloud providers seek to deny disruption at the user-end. The ultimate goal is to close off 'the very possibility of spaces and times' (Graham and Thrift, 2007: 11) when client data is not accessible, with the aim of producing a 'world without events' (Masco, 2014: 31) for their clients. That is, a world in which device malfunction, obsolescence, theft or upgrades are barely experienced as disruptions because clients can simply access their data from another device or quickly re-install their data on new systems. Working to ensure that device failure does not result in data loss, cloud providers strive to reconfigure breakdowns and malfunctions into uneventful and forgettable moments, rather than traumatic or catastrophic data loss events.[14] This has implications for how we think about and theorise failure in relation to digital technologies.

It has long been a commonplace in analyses of human-machine relations that the failure of technological objects, systems or tools is a disruptive event. Stemming from Heidegger's (1962) philosophy of technology, it has been widely theorised that, in their moments of malfunction, technologies shift status from being almost-invisible tools that facilitate work into stubborn and unruly objects that disrupt routines or habits (Verbeek, 2004: 79; Harman, 2009). If technologies – from computer systems to infrastructures – are designed to disappear into the background of everyday life, upon breakdown, they forcefully reappear. This moment of reappearance via breakdown has been of great interest to social theorists because it provides an opening onto complex and fragile relations between people, technology and the industries that design and provision them – relations that are concealed or go unnoticed when the system is working smoothly.[15] From this perspective, failure and breakdown are valuable revelatory moments (and valuable analytical opportunities) precisely because they are understood as exceptional, disruptive events rather than normal operating states, through which we can therefore learn something new about our world. This line of thinking has perhaps been most prominent in disaster studies scholarship, in which disasters are valuable precisely because they are not the norm but 'messy times when norms […] fail' and which therefore provide a momentary window

[14] Of course, the extent to which device failure is considered catastrophic depends not only on the data lost, but also on the sentimental or financial value of the lost, broken or stolen device itself.

[15] Recent work from infrastructure studies scholars and historians of technology has begun to move analyses of technology failure beyond the 'invisible until breakdown' paradigm developed by Susan Leigh Star (1999), exploring shifting layers of (in)visibility (Furlong, 2020) through a focus on those whose work revolves around practices of maintaining, fixing and repairing (Denis and Pontille, 2014; Russell and Vinsel, 2018; Mattern, 2018; Graziano and Trogal, 2019)

through which we can 'analytically denaturalise and examine these practices that create norms' (Petersen cited in Guggenheim, 2014: 7).

But what happens when failure becomes the norm? What happens when failure 'fails' to disrupt, to produce new knowledge or to register as an 'event'? Arjun Appadurai and Neta Alexander (2020: 120) have recently suggested that, given the regularity with which digital technologies freeze, crash and breakdown, the relationship between failure and knowledge production itself begins to breakdown. '[O]ur technological failures', they suggest, 'do not teach us something new about our world; their repeated breakdowns do nothing more than further obstruct the underlying logic and hidden infrastructures that sustain them' (ibid.). These 'hidden infrastructures' themselves might work to render failure non-disruptive and non-revelatory, as with the cloud. Indeed, if, for Appadurai and Alexander, it is the regularity of device breakdown that renders failure ordinary rather than revelatory, the cloud further obfuscates and limits the subversive capacity of failure by absorbing the disruptive or traumatic impact of data loss that might otherwise accompany routine device malfunction. With its promise to ensure data is safe and instantly downloadable, the cloud works to reduce and deny moments of IT disruption and to increase digital productivity by ensuring that work need not stop when a device malfunctions but can simply be picked up again from another device.

This is not to say that the cloud always delivers on its techno-productive promise of uninterruptible data continuity. Indeed, while working to render failure forgettable it also produces new opportunities for disruption. With users working from documents stored in the cloud, loss of Internet connectivity can mean loss of access to these documents. While working to conceal routine, run-of-the-mill failure events, the 'infrastructural excess' (Taylor, 2018) of cloud storage also increases the potential for large-scale, cascading failures. As Hu (2015: 98) observes, 'one cloud server fails to synch with another, or one network's router misfires, causing a chain of errors that ripple through all other interconnected networks'. A good example of such an event occurred in May 2017 when British Airways' (BA) primary and standby data centres in London both failed, resulting in a series of domino-like server crashes that were described in the data centre press as a 'contagion [that] spread around the world and grounded all BA flights at the height of the failure' (Corfield, 2017). During such moments of disruption the cloud fantasy of seamless continuity fails. Here we see that the 'world-disclosing properties of breakdown' (Jackson, 2014: 230), have not entirely been sealed off by the cloud, but redistributed and rescaled.

Conclusion: Economies of failure and preparedness

The cloud is an infrastructure that is made through and for the failure of digital technology. Underpinning the growing adoption of cloud-based back-up solutions is an awareness and anticipation of the anytime-anywhere potential of digital devices to crash or break, coupled with the need to ensure the continuous availability of data across these devices that could fail at any moment. Standing by for data loss is thus driven by a form of 'broken world thinking' (Jackson, 2014: 221), which assumes that technology failure is inevitable and requires anticipatory investments in standby from end-users and cloud providers alike to prepare for this eventuality. This form of standby involves the synchronisation of people, devices, infrastructure and back-up equipment into arrangements of preparedness for IT failure. Standing by for data loss thus provides a salient example of the anticipatory subject positions and practices that have been identified as a defining quality of our current historical and political moment (Adams et al., 2009; Anderson, 2010; Harvey et al., 2013).

Since the mid-twentieth century, data loss has arisen within digital capitalism as both a source of 'threat and opportunity, danger and profit' (Anderson, 2010: 782), generating new imaginaries of data-based disaster and profitable new industries dedicated to data preparedness. Today, for technology behemoths like Microsoft, Apple and Google, all of whom now offer cloud-based back-up space for a monthly subscription, cloud storage is becoming a key strategic tool in the long game for revenue growth (Gartenberg, 2019). As users generate increasingly large volumes of data through their devices, their cloud storage needs for these ever-accumulating personal digital archives will continue to grow over their lifetimes, as will the cloud subscription fees. While a few gigabytes of introductory cloud storage space are often provided for free, the costs for additional storage can quickly become expensive.

By separating data from the fragile materiality of digital devices, cloud providers promise their clients a form of transcendental and perpetual data storage that will last indefinitely into the future, from 'next year' to 'next century' (Eggers, 2013: 43). Different scales of digital time are at work here. If digital commodities are defined by their rapid obsolescence, the cloud offers a longer-term temporality that transcends the lifespan of the device. Smartphones, tablets and laptops are thus valuable tools with which technology companies can lock users into their cloud service, converting owners of time-limited devices into potentially lifelong cloud-customers within tightly integrated brand ecosystems. At the time of writing this essay, there is no 'switching service' that enables users to quickly and easily transfer their data between cloud providers who may offer better rates or security.

Striving to render IT failure as uneventful, non-disruptive and forgettable as possible, the cloud props up and supports the continuity of a techno-economic system based on the continuous failure and upgrading of devices. By making it quick and easy for users to simply re-download their system data to a new device, rather than change the sociotechnical and economic conditions that culminate in the recurrent crises of device failure in the first place, the cloud facilities the rapid turnover of digital electronics, further reinforcing business and marketing models based around logics of planned obsolescence and perpetual upgrading. In this sense, standby might be understood as an anticipatory form of maintenance-work that serves to sustain existing socioeconomic orders (Russell and Vinsel, 2018: 7; Sims, 2017). When failure becomes regular and intentional (as an 'engineered' or 'planned' design strategy of digital technologies) it requires labour and infrastructure to render it tolerable. This is where the cloud, as a dedicated infrastructure of data preparedness, steps in. The cloud and the device must thus be seen as two parts of a self-perpetuating economy of data preparedness and technological failure. IT failure becomes something to be managed and maintained, a precarity that we must learn to live with and constantly stand by for, if we don't want to lose our data.

references

Adams, V., M. Murphy and A.E. Clarke (2009) 'Anticipation: Technoscience, life, affect, temporality', *Subjectivity*, 28(1): 246-265.

Alexander, N. (2017) 'Rage against the machine: Buffering, noise, and perpetual anxiety in the age of connected viewing', *Cinema Journal*, 56(2): 1-24.

Anderson, B. (2010) 'Preemption, precaution, preparedness: Anticipatory action and future geographies', *Progress in Human Geography*, 34(6): 777-798.

Appadurai, A. and N. Alexander (2020) *Failure*. Cambridge: Polity Press.

Beniger, J. (1986) *The control revolution*. Boston, Massachusetts: Harvard University Press.

Bennett, J. (2005) 'The agency of assemblages and the North American blackout', *Public Culture*, 17(3): 445-465.

Bratton, B.H. (2015) *The stack: On software and sovereignty.* Cambridge, Massachusetts: MIT Press.

Burrell, J. (2012) *Invisible users: Youth in the internet cafes of urban Ghana.* Cambridge, Massachusetts: MIT Press.

Carroll, T., D. Jeevendrampillai, A. Parkhurst and J. Shackelford (eds.) (2017) *The material culture of failure: When things do wrong*. London and New York: Bloomsbury.

Castells, M. (1996) *The rise of the network society*. Oxford: Blackwell.

Cavelty, M.D. (2008) *Cyber-security and threat politics: US efforts to secure the information age.* London: Routledge.

Chandler, D. and J. Reid (2016) *The neoliberal subject: Resilience, adaptation and vulnerability.* London and New York: Rowman and Littlefield International.

Chun, W. (2016) *Updating to remain the same: Habitual new media*. Cambridge, Massachusetts: MIT Press.

Collier, S.J. and A. Lakoff (2010) 'Infrastructure and event: The political technology of preparedness', in B. Braun and S. Whatmore (eds.) *Political matter: Technoscience, democracy and public life*. Minneapolis: University of Minnesota Press.

Collier, S.J. and A. Lakoff (2015) 'Vital systems security: Reflexive biopolitics and the government of emergency', *Theory, Culture & Society*, 32(2): 19-51.

Corfield, G. (2017) 'BA IT systems failure: Uninterruptible power supply was interrupted'. [https://www.theregister.co.uk/2017/06/02/british_airways_data_centre_configuration]

Davis, M. (2002) *Dead cities and other Tales*. New York: The New Press.

Denis, J. and D. Pontille (2014) 'Maintenance work and the performativity of urban inscriptions: The case of Paris subway signs', *Environment and Planning D*, 32(3): 404-416.

Driscoll, K. (2012) 'From punched cards to "big data": A social history of database populism', *Communication + 1*, 1(4): 1-33.

Edwards, P.N. (1998) 'Y2K: Millennial reflections on computers as infrastructure', *History and Technology*, 15: 7-29.

Eggers, D. (2013) *The Circle*. London: Hamish Hamilton.

Ernst, W. (2019) 'Archival metahistory and inhuman memory', in S.K. Frank and K.A. Jakobsen (eds.) *Arctic archives: Ice, memory and entropy*. Bielefeld: Transcript Verlag.

Furlong, K. (2021) 'Geographies of infrastructure II: Concrete, cloud and layered (in)visibilities', *Progress in Human Geography*, 45(1):190-198.

Gabrys, J. (2013) *Digital rubbish: A natural history of electronics.* Ann Arbor: The University of Michigan Press.

Garrett, B. (2020) 'Doomsday preppers and the architecture of dread', *Geoforum*, doi: 10.1016/j.geoforum.2020.03.014.

Gartenberg, C. (2019) 'How Apple makes billions of dollars selling services', *The Verge*, 20 March. [https://www.theverge.com/2019/3/20/18273179/apple-icloud-itunes-app-store-music-services-businesses]

Glanz, J. (2012) 'The cloud factories: Power, pollution and the Internet' [https://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html].

Graham, S. and N. Thrift (2007) 'Out of order: Understanding repair and maintenance', *Theory, Culture & Society*, 24(3): 1-25.

Graham, S. (2010) 'When infrastructures fail', in S. Graham (ed.) *Disrupted cities: When infrastructure fails*. London and New York: Routledge.

Graham, S. (2015) 'Stealth architectures and the geographies of back-up', in A. Fard and T. Meshkani (eds.) *New Geographies 7*. Boston: Harvard Graduate School of Design.

Graziano, V. and K. Trogal (2019) 'Repair matters', *ephemera*, 19(2): 203-227.

Greenpeace (2012) *How clean is your cloud?* Amsterdam: Greenpeace International.

Grove, K. (2016) 'Disaster biopolitics and the crisis economy', in J.L. Lawrence and S.M. Wiebe (eds.) *Biopolitical disaster*. London and New York: Routledge.

Guggenheim, M. (2014) 'Introduction: Disasters as politics – politics as disasters', in M. Tironi, I. Rodríguez-Giralt and M. Guggenheim (eds.) *Disasters and politics: Materials, experiments, preparedness*. Chichester, West Sussex: Wiley Blackwell.

Gustin, J.F. (2010) *Disaster and recovery planning: A guide for facility managers* (fifth edition). Lilburn, Georgia: The Fairmont Press.

Harman, G. (2009) 'Technology, objects and things in Heidegger', *Cambridge Journal of Economics*, 34(1): 17-25.

Harvey, P., M. Reeves and E. Ruppert (2013) 'Anticipating failure: Transparency devices and their effects', *Journal of Cultural Economy*, 6(3): 294-312.

Harvey, P. and H. Knox (2015) *Roads: An anthropology of infrastructure and expertise*. Ithaca: Cornell University Press.

Heidegger, M. (1962) *Being and time*, trans. J. Macquarrie and E. Robinson. New York: Harper and Row.

Henke, C.R. (1999) 'The mechanics of workplace order: Toward a sociology of repair', *Berkeley Journal of Sociology*, 44: 55-81.

Herbane, B. (2010) 'The evolution of business continuity management: A historical review of practices and drivers', *Business History*, 52(6): 978-1002.

Herman, C.F. (1963) 'Some consequences of crisis which limit the viability of organisations', *Administrative Science Quarterly*, 12: 61-82.

Hogan, M. (2015) 'Data flows and water woes: The Utah Data Center', *Big Data & Society*, 2(2): 1–12.

Holt, J. and P. Vonderau (2015) '"Where the Internet lives": Data centers as cloud infrastructure', in L. Parks and N. Starosielski (eds.) *Signal traffic: Critical studies of media infrastructures*. Urbana, Chicago, and Springfield: University of Illinois Press.

Hu, T. (2015) *A prehistory of the cloud*. Cambridge, Massachusetts: MIT Press.

Huddleston, C. (2016) '"Prepper" as resilient citizen: What preppers can teach us about surviving disaster', in M. Companion and M.S. Chaiken (eds.) *Responses to disasters and climate change: Understanding vulnerability and fostering resilience*. Boca Raton: CRC Press.

Jackson, S.J. (2014) 'Rethinking repair', in T. Gillespie, P.J. Boczkowski and K.A. Foot (eds.) *Media technologies: Essays on communication, materiality, and society*. Cambridge, Massachusetts and London: MIT Press.

Keck, F. (2016) 'Preparedness' Theorizing the Contemporary, *Fieldsights*, September 30. [https://culanth.org/fieldsights/preparedness].

Klein, N. (2007) *The shock doctrine: The rise of disaster capitalism*. New York: Metropolitan Books.

Lakoff, A. (2006) 'Techniques of preparedness', in T. Monahan (ed.) *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.

Lakoff, A. (2008) 'The generic biothreat, or, how we became unprepared', *Cultural Anthropology*, 23(3): 399-428.

Larkin, B. (2013) 'The politics and poetics of infrastructure', *Annual Review of Anthropology* 42: 327–343.

LeBel, S. (2012) ‘Wasting the future: The technological sublime, communications technologies and e-waste’, *Communication +1*, 1(1): 1-19.

Lutz, C. (1997) ‘Epistemology of the bunker: The brainwashed and other new subjects of permanent war’, in J. Pfister and N. Schnog (eds.) *Inventing the psychological: Toward a cultural history of emotional life in America*. New Haven and London: Yale University Press.

Mahoney, M.S. (1998) ‘The history of computing in the history of technology’, *IEEE Annals of the History of Computing*, 10(2): 113-125.

Mantz, J. (2008) ‘Improvisational economies: Coltan production in the eastern Congo’, *Social Anthropology*, 16(1): 34–50.

Masco, J. (2014) *The theatre of operations: National security affect from the Cold War to the war on terror.* Durham, North Carolina: Duke University Press.

Mattern, S. (2016) ‘Cloud and field’ [https://placesjournal.org/article/cloud-and-field/].

Mattern, S. (2018) ‘Maintenance and care’ [https://placesjournal.org/article/maintenance-and-care/].

McKinney, C. and D. Mulvin (2019) ‘Bugs: Rethinking the history of computing, *Communication, Culture & Critique*, 12: 476-498.

McMillan, R. (2012) ‘Guns, squirrels and steel: The many ways to kill a data center’ [https://www.wired.com/2012/07/guns-squirrels-and-steal].

Mills, M.F. (2018) ‘Preparing for the unknown unknowns: “Doomsday” prepping and disaster risk anxiety in the United States’, *Journal of Risk Research*, 22(10): 1267-1279.

Mosco, V. (2014) *To the cloud: Big data in a turbulent world*. Boulder: Paradigm Publishers.

Nield, D. (2015) ‘How to replace your external hard drive with cloud storage’ [https://www.t3.com/news/how-to-replace-your-external-hard-drive-with-cloud-storage].

Parks, L. (2007) ‘Falling apart: Electronics salvaging and the global media economy’, in C.R. Acland (ed.) *Residual media*. Minneapolis: University of Minnesota Press.

Ponemon Institute (2016) 'Cost of data Center outages' [https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf].

Radding, A. (1999) 'The great tape hunt', *Infoworld*, 21(15): 3-8.

Ribes, D. and T.A. Finholt (2009) 'The long now of technology infrastructure: Articulating tensions in development', *Journal of the Association for Information Systems*, 10: 375-398.

Rochlin, G.I. (1997) *Trapped in the net: The unanticipated consequences of computerisation*. Princeton, New Jersey: Princeton University Press.

Russell, A.L. and L. Vinsel (2018) 'After innovation, turn to maintenance', *Technology and Culture*, 59(1): 1-25.

Russell, A.L. and L. Vinsel (2020) *The innovation delusion: How our obsession with the new has disrupted the work that matters most.* New York: Random House.

Schüll, N.D. (2018) 'Digital containment and its discontents', *History and Anthropology*, 29(1): 42-48.

Sims, B. (2017) 'Making technological timelines: Anticipatory repair and testing in high performance scientific computing', *Continent*, 6(1): 81-84.

Smith, S. (2015) 'The real cost of data loss and how to prevent it' [http://techgenix.com/real-cost-data-loss-and-how-prevent-it].

Star, S.L. and K. Ruhleder (1994) 'Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems', *Proceedings of the conference on computer supported cooperative work*, Chapel Hill, ACM Press.

Star, S.L. (1999) 'The ethnography of infrastructure', *American Behavioral Scientist*, 43(3): 377-391.

Starosielski, N. (2015) *The undersea network*. Durham and London: Duke University Press.

Taylor, A.R.E. (2018) 'Failover architectures: The infrastructural excess of the data centre industry' [https://failedarchitecture.com/failover-architectures-the-infrastructural-excess-of-the-data-centre-industry/].

Taylor, A.R.E. (2019) 'The data centre as technological wilderness', *Culture Machine*, 18.

Taylor, A.R.E. (2021) 'Future-proof: Bunkered data centres and the selling of ultra-secure cloud storage', *Journal of the Royal Anthropological Institute*, doi: 10.1111/1467-9655.13481.

Taylor, A.R.E. and J. Velkova (2021) 'Sensing Data Centres', in N. Klimburg-Witjes, N. Poechhacker and G.C. Bowker (eds.) *Sensing in/security: Sensors as transnational security infrastructures*. Manchester: Mattering Press.

Trovalla, E. and U. Trovalla (2015) 'Infrastructure turned suprastructure: Unpredictable materialities and visions of a Nigerian nation', *Journal of Material Culture*, 20(1): 43-57.

Velkova, J. (2016) 'Data that warms: Waste heat, infrastructural convergence and the computation traffic commodity', *Big Data & Society*, July-December: 1-10.

Verbeek, P. (2004) *What things do: Philosophical reflections on technology, agency and design*. University Park: Pennsylvania State University Press.

Virilio, P. (2007) *The original accident*. Cambridge: Polity Press.

Zuboff, S.S. (1988) *In the age of the smart machine: The future of work and power.* New York: Basic Books.

the author

A.R.E. Taylor is an anthropologist based at the University of Cambridge. He works at the intersection of social anthropology, media archaeology and the history of technology. His research concentrates on imaginaries of digital collapse and on the material and temporal dimensions of data storage and security. He is an Editorial Assistant for the *Journal of Extreme Anthropology* and a founder of the Cambridge Infrastructure Resilience Group, a network of researchers exploring critical infrastructure protection in relation to global catastrophic risks. He is also a founding member of the Social Studies of Outer Space (SSOS) Research Network. His research interests include: data futures, digital preservation, outer-space, techno-apocalyptic narratives and pre-digital nostalgia.
Email: aret2@cantab.ac.uk
Twitter : @alexretaylor