Are insolvency laws ready for digital service failures?

Rebecca Parry looks at the problems surrounding the insolvency of digital services and the tensions they bring

REBECCA PARRY
Professor, Nottingham Law School, Nottingham Trent University [1]

> ***Important service providers are gaining benefits from the scalability and costs savings of cloud computing, yet the risks of operating in this way have received limited attention.***

Recent years have seen increasing reliance on digital services, trends accelerated by the Covid-19 pandemic and working from home.[1]

Government services, banks and other important service providers are gaining benefits from the scalability and costs savings of cloud computing, yet the risks of operating in this way have received limited attention. As well as cloud computing, the digital infrastructure subsector includes top-level domain name registries,[2] domain name services[3] and internet exchange points.[4] These services are vital to the proper functioning of the internet, yet they are commonly provided by nonstate enterprises which carry the same risks of failure as other firms in competitive markets.

Despite wide existing recognition of the importance of digital services in modern society and the strong pro-active arrangements in measures such as the EU's Network and Information Systems Regulations 2018 SI 2018/506, there is no special provision for the handling of the affairs of insolvent digital service suppliers.[5] There is, however, potential for a significant public impact in the event of an insolvency of a digital service provider. Dependence on a few key providers of digital services brings the possibility of a "too big to fail" scenario[6] and, as with the 2007-8 banking crisis, the possibility of problems caused by a lack of knowledge of the technologies that we rely on. Like the banks, there is the potential for contagion in concerns about a digital service business and a "run on the banks" scenario might arise.[7] The complex and highly-connected nature[8] of digital services can also make risks difficult to assess. Moreover, users tend to be unaware of the underlying technologies that they use every day[9] nor the potential hazards that would be presented by the failure of a company supplying services via these technologies. Reliance on a small number of suppliers also presents the prospect of cybersecurity weaknesses and exploitation by hackers, which is one way in which a crisis in this area could be sparked.[10]

The wide-ranging importance of digital services can be exemplified by cloud computing services. In a study by the insurer Lloyd's of the potential impact of cloud computing failures on the US market, it was found that an outage of a cloud service provider for even a few days would impact significantly on manufacturing, wholesale and retail trade, information services, finance and insurance and transportation and warehousing, with MSMEs carrying a larger share of the losses.[11] Disruption to digital services would also impact on individuals, given the importance of the internet to modern working and keeping in touch with friends and family. The outage at the content delivery network.[12] Fastly in June 2021, which disrupted government services as well as services from companies, was an illustration of the significant impact that even a one-hour loss of service at one company can bring.[13] Although outages are rare and there are good failure prevention approaches in this sector, the banking crisis demonstrated that failures are possible even in highly regulated sectors. Digital service failures are likely to be messy to resolve, given the lean staffing structure of many digital service providers and a likely high volume of demands from customers. In the UK in 2013, a data centre, 2e2, failed leaving customers with expensive costs for the recovery of their content (around £1 million), a process that was anticipated to take 16 weeks.[14] More recently, there have been high profile and complex failures in the cloud computing sector including examples involving government services.[15]

These problems can lead to a **tension at the heart of digital service insolvencies**, since insolvency laws primarily provide a framework for the resolution of claims of creditors in an orderly fashion. Laws are typically designed to enable creditors to be repaid efficiently and at a limited cost, yet some limited period of continued operation is in the interests of customers of digital service suppliers, since customers will want to recover their content and source alternative providers before the service is shut down. In this context, as noted, a variety of issues are likely to add complexity, which may be time-consuming to resolve. Where the service provider is viable, restructuring laws may enable a loss of service to be averted, but greater difficulties are likely where the service provider is not a suitable candidate for restructuring. Liquidation laws are commonly designed to enable a swift closure of the debtor's affairs and there may be limited sums for continued trading. This raises the

Table 1: Examples of *ex ante* and *ex post* approaches in cases of potentially wide public

	Ex Ante – failure prevention	Ex Post – protection of functions (sometimes entities)
Banking	Highly regulated. Controls on entry, customer deposit safeguards etc.	Includes specialist restructuring laws and customer deposit protections.
P2P Crowdfunding	Highly regulated. Requirement of Financial Conduct Authority authorization. Safeguards.	Required wind-down arrangements
Airlines	Highly regulated, domestically and internationally.	Customer compensation. Ad hoc protection of functions e.g., Monarch, Thomas Cook customer repatriation.
Energy suppliers	Highly regulated. Gas Act 1986, s 7A licensing system. Fit and proper requirement, customer safeguards, requirements of financial responsibility etc.	UK special administration regime. Protection of functions through appointment of supplier of last resort and transfer of customers to new suppliers.

question of whether there should be a sector-specific approach to insolvencies in the digital services sector. In other sectors, shown in the table above, which mostly considers the UK position, there are other sectors where the prospect of failure is addressed, recently seen in the UK approach in handling failures of energy suppliers.

One challenge for a centralised approach to digital service insolvencies is likely to be the creation of a funding structure that avoids recourse to public funds, as far as possible, in the managed closedown of digital economy service suppliers. Funding was an issue that was considered in the UK review of airline insolvencies,[16] and, although that is a quite different context, it reviewed key principles that can inform the approach to digital economy insolvencies. A levy on digital service suppliers would be one possibility that could enable insolvencies to be handled in a way that minimises the impact on customers.

Conclusion

The rise in energy costs is likely to impact heavily on digital service companies, which use large volumes of electricity. There have already been failures in this sector and more can be expected. Given the growing levels of reliance on digital services, there should be consideration of whether an approach for this sector which anticipates the prospects of insolvencies can be developed.

To be continued. ■

Footnotes:

1 This article builds on Rebecca Parry, "An Insolvency Regime to Support the Digital Economy", paper given at Forward Thinking - A Research and Technical Conference (Insolvency Service), available at: <https://sites.google.com/view/forwardthinkingconference2021/home?pli=1>. The first part provides a UK domestic perspective. The second part of this article will consider in further detail how these cases might be handled internationally and will be published in one of the next editions of Eurofenix.

2 These businesses handle the reservation of domain names as well as the assignment of IP addresses for those domain names. It can be regarded as a type of property register. For example .com names are controlled by Verisign.

3 The website's IP (internet protocol) address, which would otherwise be an unmemorable string of numbers, is converted into a more recognisable and memorable name by the DNS. It can be regarded as a phone book. See e.g., Cloudflare, "What is DNS", available at: <https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/>.

4 IXPs are part of the internet infrastructure, acting as points to connect and exchange internet traffic in more efficient ways. See e.g., Internet Society, "Explainer: What is an Internet Exchange Point (IXP)?" (22 June 2020), available at: <https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/>.

5 Special administration procedures are provided in respect of various industries where companies carry out public functions e.g., in water or energy, as considered below.

6 Acknowledged by Lloyd's, "Cloud Down, Impacts on the US Economy, Emerging Risk Report 2018", available at: <https://www.lloyds.com/clouddown>; Rana Faroohar, "How big tech is dragging us towards the next financial crash" (Guardian, 8 November 2019); Rana Faroohar, Don't Be Evil: the Case Against Big Tech (Penguin, 2019), Chapter 10.

7 European Network and Information Security Agency, "Cloud Computing, Benefits, Risks and Recommendations for Information Security" (December 2012), 19.

8 Services are often layered. For example, Amazon Web Services cloud infrastructure is used by the cloud-based platform provider Heroku and by Netflix, which provides software to view entertainment content.

9 Joe McKendrick, Most Americans Don't Understand Cloud Computing; Does It Really Matter? (Forbes, 29 August 2012).

10 David Wall, "Fastly's global internet meltdown could be a sign of things to come" (The Conversation, 9 June 2021), available at: <https://theconversation.com/fastlys-global-internet-meltdown-could-be-a-sign-of-things-to-come-162390>.

11 Lloyd's (above note 6).

12 The role of a CDN is to speed up internet transactions using proxy servers. CDNs are geographically dispersed and enable faster content delivery by bringing service provision closer to customers.

13 Neil Miller, "Inside the Fastly Outage: a Firm Reminder on Internet Redundancy" (Data Center Dynamics, 22 June 2021), available at: <https://www.datacenterdynamics.com/en/opinions/inside-the-fastly-outage-a-firm-reminder-on-internet-redundancy/>.

14 Computer Weekly, "2e2 datacentre administrators hold customers' data to £1m ransom" (8 Feb 2013), available at: <https://www.computerweekly.com/news/2240177744/2e2-datacentre-administrators-hold-customers-data-to-1m-ransom>.

15 Insolvency Service, "Virtual Infrastructure Group Limited and UKCloud Limited: information for creditors and interested parties" (25 October 2022), available at: <https://www.gov.uk/government/news/virtual-infrastructure-group-limited-and-ukcloud-limited-information-for-creditors-and-interested-parties>.

16 Airline Insolvency Review (chaired by Peter Bucks), Final Report (March 2019).

> ***One challenge for a centralised approach to digital service insolvencies is likely to be the creation of a funding structure that avoids recourse to public funds***