"The Post Office scandal highlights the dangers of accepting without question the output of automated systems as reliable evidence" Dr Sam De Silva, Technology Partner at international law firm CMS

The Tip of the Iceberg

As the Public Inquiry into the Post Office Scandal continues, **The Rt Hon. Sir Oliver Letwin** is calling for a fallback system to help resolve situations where computer systems, presumed to be infallible, turn out to be less so. He talked to **Fergus Byrne.**

Although he doesn't know if he will be called to give evidence at the Public Inquiry into what is now known as the "Post Office Scandal". The Right Honourable Sir Oliver Letwin sees the whole sorry saga as a wake-up call for a 'Plan B' on how to deal with the dangers of our over-reliance on technology.

Oliver was one of a small group of MPs who first brought the now infamous Post Office miscarriage of justice to light. After one of his constituents came to see him about their experience with the company's Horizon computer system, he mentioned it to fellow MP James Arbuthnot who already had experience of the growing problem through one of his constituents, Jo Hamilton. Oliver recalls how everyone had so much less experience of computers in those days, and especially of them 'going bananas'. He suggested to James, now Lord Arbuthnot, that they go and speak to the chair and chief executive of the Post Office, but remembers it as coming up against 'a blank wall'.

Out of that emerged a series of meetings with other MPs who'd had similar experiences and eventually the Post Office agreed to appoint forensic accountants, Second Sight, to independently investigate what was going on. When Second Sight's investigations uncovered problems with the software system, they found the Post Office less keen for the investigation to continue. More than 900 subpostmasters and postmistresses were prosecuted for stealing money because of incorrect information provided by the computer system which had been supplied to the government-owned Post Office by Fujitsu UK. Although Oliver's constituent was never convicted of any offences, he believes that 'really considerable damage was done to her.'

The rest of the story is well documented by journalists at *Computer Weekly*, *Private Eye* and by investigative journalist Nick Wallis for *Panorama* and his own blog. Nick is starting a tour telling the story at the Marine Theatre, Lyme Regis in March. For more on his view of the enormous issues now facing the Post Office, the software developer Fujitsu and the Government, visit www.marshwoodvale.com and read his interview in our February issue. This story is also well recounted in the ITV drama *Mr Bates vs The Post Office*.

However, even though this particular 'computer problem' has turned out to be widespread across the United Kingdom, it is not isolated to one software system, nor to one industry. And is therefore, warns Oliver Letwin, not by any means the end of the story.

There have been many high-profile issues, from coding errors to hacking attempts over the years that have had profound effects. One example is the Knight Capital Group stock trading debacle in 2012. Due to a coding error in the company's trading software, they inadvertently bought and sold millions of shares in just 45 minutes, causing a loss of $440 million and forcing the company to seek a bailout.

In 2011, a software error at the Royal Bank of Scotland (RBS) caused a technical meltdown, leaving millions of customers unable to access their accounts for several days.

The bank faced heavy criticism and was forced to pay out millions in compensation to affected customers.

In 2017, a major computer error at British Airways led to the cancellation of hundreds of flights, affecting over 75,000 passengers. Also in 2017, the WannaCry ransomware attack affected over 200,000 computers in 150 countries, including those used by the NHS, leading to cancelled appointments, delayed surgeries, and a significant impact on patient care.

In another shocking experiment, *Wired* journalist, Andy Greenberg, once took part in a test of car hacking. His car was remotely hacked while he was behind the wheel. As he drove, the hackers started to take control of the car, activating air vents and windshield wipers. Next, the transmission was cut and finally, they remotely activated the brakes. Even though Andy tried to control his car, the hackers had more power. The experiment uncovered issues which were later fixed.

These are just a few examples that made it into mainstream news. The issue for Oliver Letwin is that we have no 'Plan B' when it comes to automated transactions. The Post Office scandal may well be the tip of the iceberg showing the substantial impact that computer errors can have on businesses and people's lives.

From banking to utility payments, and travel to parking, we are now reliant on automated systems that make it very hard to resolve when there are errors. Oliver sees the benefit of simple systems, but points out that 'once computers get to be involved in very complex affairs, very complex programmes with many thousands, millions, billions, trillions of interactions, it becomes quite possible for particular interactions to cause particular problems.' Problems that may not be immediately obvious to the user.

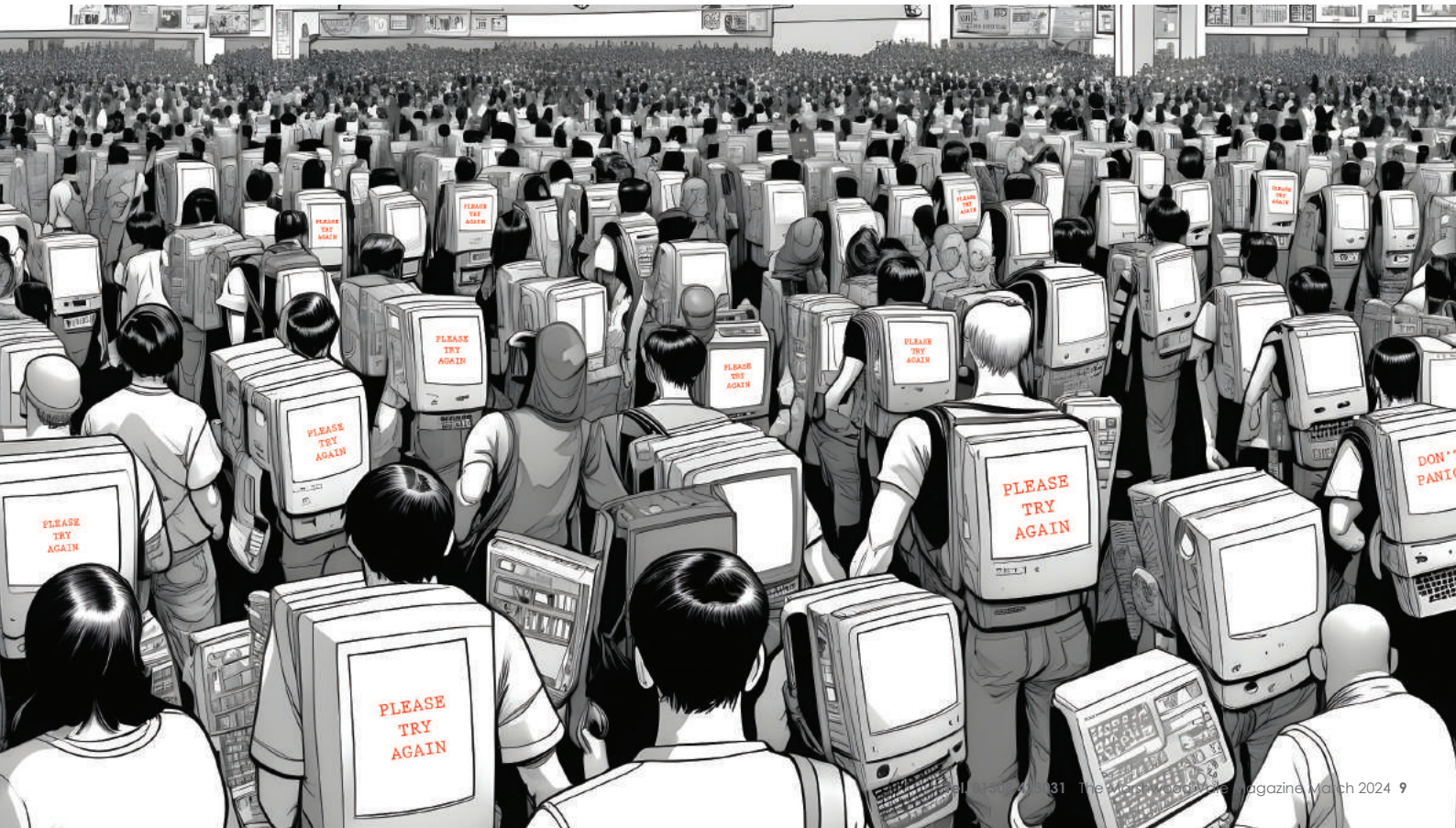
Many of us have had a situation where we have tried to complete a transaction online and been told the process hasn't worked and been told to 'Please try again'. Oliver described how one postmaster's system had repeatedly told him a transaction hadn't gone through—when in fact it had—causing a massive overpayment.

Purchasing tickets for a holiday, Oliver found the same thing happened to him. The system told him the transaction hadn't gone through so he completed it again, only to find he had been billed twice for the same seats, with the same names, on a flight to Europe. He was fortunate to be able to speak to someone at the company who saw immediately the error and rectified it.

But this is where the problem, and the lack of a 'Plan B' lies. We all know how difficult, time-consuming and frustrating it is to try to contact someone who can help when automated transactions don't work. Dealing with computers in these situations, Oliver says, is sometimes 'like talking to someone who's slightly vague or who's disconcerted by something, or who's suffering from a bad cold, or has Alzheimer's.' However, as automated systems become more and more ingrained in our lives, a method of resolving problems becomes more and more important. Especially when the law still presumes the computer is right.

The frightening thing that the Post Office scandal highlights is that the computer isn't always right. However, the law still presumes the computer can be relied on and that the 'presumption' of its correctness should stand up in court. In light of the Post Office scandal, BCS, the Chartered Institute for IT, has called for an end to the legal presumption that 'computer systems data are always correct, with no burden on the prosecution to prove it.'

Dr Sam De Silva, Partner at international law firm, CMS and Chair of BCS' Law Specialist Group has said: 'The Post Office scandal highlights the dangers of accepting without question the output of automated systems as reliable evidence. There is currently a legal presumption that the computer is always right; the Post Office could



rely on the fact that the courts assumed the system to be functioning well.'

Oliver Letwin is aware of this and believes that such a 'presumption' is now under review. 'The problem is that that's clearly outdated' he says. 'I mean, as the deep fake cases show, as these Post Office cases show, any number of cases will show, you can't start with that presumption. Any more than you can start with the presumption that the human being would have made a mistake. Computers are just as likely as human beings to make mistakes once they get to be very complicated.'

And the degree of complexity that generates the possibility of what Oliver calls 'the bizarre', he says, is hugely multiplied by the fact that 'you're not talking here about a computer, you're talking about a network of computers and networks of networks. So that there may be millions or even billions of machines interacting to produce the particular results you're seeing. And so the "presumption" that whatever it is you're expecting to come out, will have come out of it on a given occasion, is ludicrous.'

resulted in catastrophic failures in infrastructure on many levels, Oliver points out that our reliance on the internet for communication, for example, leaves us very vulnerable. In light of the Post Office and the many other computer problems that have remained under the public radar, we have all become massively over-reliant on technology to run our lives.

The only protection we can have against systemic failure, 'in the sense of everything just sort of collapsing' he says, 'is actually to have fallback options which are not modern and sophisticated.' He knows they aren't going to be as financially efficient as modern sophisticated systems. 'A map instead of GPS, a record of names and addresses on a piece of paper in a filing cabinet rather than on a computer. And human beings to talk to, to get things sorted out.'

These old methods are massively inefficient and probably not financially ideal for businesses that want to maximise profits by reducing workforce. But Oliver says 'We have to be able to fall back on [these systems] in order to protect ourselves against the possibility of a whole system that just doesn't work for a while. Similarly, when we're

'It's very difficult for a local postmaster to make £50,000 just sort of disappear into thin air. Now, it's one thing for a drug cartel to do this, but it's just awfully difficult for a postmaster or postmistress.'

Using the Post Office as an example of the dangers of overreliance on automation and the presumption that the computer is always right, he points out how in the days before computer networks there was never a situation where hundreds of employees were found to be stealing at the same time. 'As far as we know, there had not been any particular suggestion of widespread miscarriages of justice under those arrangements.'

He believes we need to go back to having the option of 'old-fashioned sleuthing' as a backup. In the past, he says, 'People would go and investigate the bank accounts of the individual and look at their lifestyles, and inquire of people that knew them whether they regarded them as honest, and all sorts of other things which are non-mechanistic.'

He says it's possible that the belief that the computer is never wrong may have influenced people at all levels of the Post Office affair. 'And I suspect that they therefore didn't do any other set of investigations that would have been a sanity check on whether their computer was telling the truth. And it's very difficult for a local postmaster to make £50,000 just sort of disappear into thin air. Now, it's one thing for a drug cartel to do this, but it's just awfully difficult for a postmaster or postmistress. So, plain old-fashioned sleuthing would probably have revealed those that were up to no good and those where the machine was telling a lie. But I suspect there wasn't an effort to do that, because people were relying on the machine.'

Which is what brings us to the need for a backup. In his book, *Apocalypse How?*, a story of how the lack of a 'Plan B' in the event of a collapse of the National Grid trying to deal with ludicrous, insanely unfair and unjust results, I think what we need to fall back on old-fashioned investigation and sleuthing and so on, and not imagine that the problem is going to be resolved by having some yet more complicated software that nobody understands.'

Anyone who has been on the waiting end of trying to resolve a computer error on a phone or utility bill will know that in the end, it is usually a sentient being that understands what has happened and not one that only answers questions from a script.

Oliver sees the human element as 'absolutely critical' to the chain of actions necessary to resolve automation issues. 'The sort of understanding of what is likely and what is not likely, as a sequence of events, that you can get by talking to a fellow human being, is an indispensable part of dealing with these things.'

He points to the 'incredible' efficiency of computer systems because they 'don't require human intervention. But actually, if you want to correct something that's gone wrong, you need a human being, because there's absolutely no way that you're going to get the computer to understand what it's done.'

Businesses, he says, are investing vast sums in computing so they don't need to employ lots of human beings. 'So you eliminate the human beings, and you thereby eliminate the one chance you actually had, not of resolving the problems, but of addressing the problems when they occur.' When what we really need is the 'inefficiency of a bank of human beings.'

And they will also need 'to have sufficient knowledge

The Post Office scandal is just one story that highlights the potential problems facing our automated world

of the things which are surrounding the person who's engaged in the transaction.' The sentient beings that are answering also need to be in the country where the problem exists. If you call to have a drain fixed and the person on the other end of the phone says 'Which country is that in? You have a problem?'

But is it plausible that large businesses will compromise on profits to resolve this sort of problem? 'I think it's entirely plausible' he says. 'I think the danger in the whole Post Office argument is that we think that after the inquiry and whatever follows—unrighteousness has been punished and innocent people have been compensated. The danger is that we think at that point—done and dusted. Not at all!' This should lead to a recognition of all that is wrong with the direction we are going.

'This is entirely addressable' he says. 'It's within the powers of governments and regulators around the world to insist, in a sensible way on the maintenance of fallback options and the maintenance of checking mechanisms, and the maintenance of complaint mechanisms.' He points out how legislation in financial services has helped protect many people from 'sharpsters' selling questionable investments. 'Because over the next 10, 20, 30, 40 years, we're going to become more and more and more dependent on these machines. And if there aren't these fallback and checking mechanisms in place, eventually governments will act, but a lot of damage will have been done.'

He believes that businesses won't set up these fallback systems on their own. It costs them money and that won't make shareholders happy. They will have to be 'forced' to do that. 'You can't expect people to do that in their own self-interest.'

It's hard to see whether legislation on the scale necessary to ensure companies invest in safety and assurance for their customers is going to be attractive to any government. However, Oliver is very aware that it will not be this government and says that perhaps 'it's the sort of thing you could imagine a Starmer government getting interested in.' In the meantime both he and James Arbuthnot and others have for some years been trying to pursue the question of incorporating 'more resilience and more fallback mechanisms' in the systems that 'we depend on' and he believes they have made some progress. And he is hopeful that informal groups, keeping the pressure up, do stand the chance of triggering 'some sort of administrative interest on the part of government.'

The Post Office scandal is just one story that highlights the potential problems facing our automated world. They include computer system errors; vulnerability to cyber-attacks; a lack of accountability; loss of human oversight and the loss of skills and knowledge. And that again may just be the tip of an iceberg that doesn't take into account the human cost.

To mitigate these risks, it's essential to maintain a balance between technological advancement and human oversight. We need safeguards, regulations, and ethical considerations to be integrated into the development and deployment of computer systems to prevent these potential consequences. Most importantly we need resilient backup systems, continuous monitoring, and robust cybersecurity measures to safeguard against the impact of system failures.

Whilst we can hope the next government takes a more active role in dealing with these problems, there may always be other, more pressing issues to attend to. But that doesn't mean we stop trying.