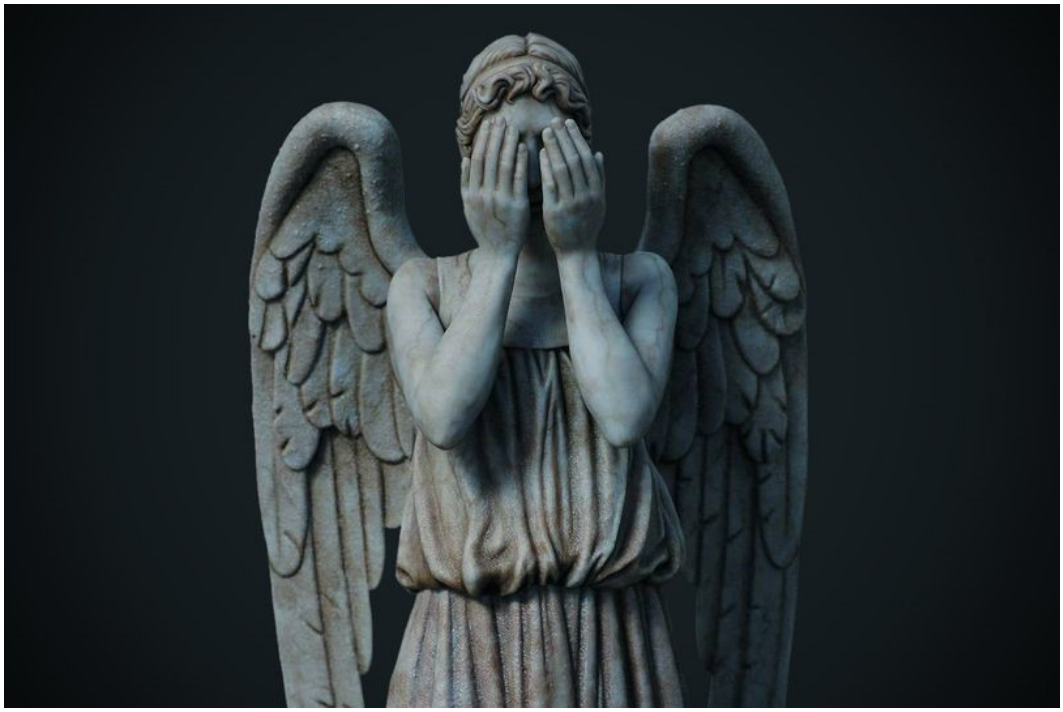
You think your gadgets serve you - but they may be serving others

We're incredibly relaxed about privacy issues... too relaxed



A Weeping Angel from Doctor Who - slightly less sinister than the CIA programme of the same name? (Image: Western Mail)

It's a dystopian nightmare. We may not be in complete control of our television sets.

The box in the corner, the magic lantern that brings the world to our living room (or any other room, for that matter) is actually watching us. Not only watching us but recording us – cataloguing our viewing habits and documenting our conversations.

In the latest dispatches from WikiLeaks, the media group that specialises in the publication of “restricted” material, it was alleged that the CIA was using Samsung TVs to spy on people.

Through a programme called Weeping Angel (and how sinister does that sound?), the US intelligence agency was allegedly able to use a television’s microphone – intended to allow voice commands – to detect and transfer information while the device appeared to be switched off.

But, as Cara McGoogan pointed out in the Daily Telegraph , this shouldn’t surprise us. Smart televisions and mobile phones are ever-present in our lives and equipped with microphones, cameras and internal memories which can used to observe and retain what we say, watch and do.

Nor is this the first time Samsung has been called to account.

In 2015 it had to respond to criticism after a report in online magazine The Daily Beast revealed that a brief passage in its privacy policy for the Interconnected SmartTV stated: “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party.”

What third party could this be?

That’s big companies willing to pay for data about consumer behaviour. In the US recently, television manufacturer Vizio settled a lawsuit brought by the US Federal Trade Commission which alleged that the company installed software on 11 million of its smart TVs to gather viewing data.

Customers were neither informed of this, nor asked for their consent for the practice to take place.

Added to this, Vizio collected each customer’s internet address and postcode, and passed this info along to companies and advertisers – whose business it is to examine consumer behaviour so that advertising can be more accurately targeted.

And it’s not just televisions and phones. In alarming news from Canada, we hear that customers who purchased a Wi-Fi enabled sex toy may be entitled to compensation because the manufacturer had been illicitly tracking the intensity of the sexual experience. In court proceedings launched by two understandably anonymous female com-

plainants, it was also alleged that the toy was able to record the date and time of use and send the information back to its server.

The fact is, as HV Jagadish, professor of engineering and computer science, notes, all our networked devices have the ability to spy on our every move and communicate in ways which we may not want them to.

As he indicates, the easily available and relatively cheap smart home monitoring kits enable the user to know how many people are in a house, in what rooms and at what times. A smart alarm clock knows what time you get up, a smart water meter knows how many times you flush the toilet. None of this is useless to advertisers seeking to build up consumer profiles.

But most of the fuss is about events in the US, right?

What have we to be afraid of in the UK?

Quite a lot, as it happens, because it's not just private companies who can harvest our data. In November last year the Investigatory Powers Act was passed without fanfare. It is, reported The Guardian , a bill that gives the UK intelligence agencies and police the most far- reaching of surveillance powers.

Ostensibly passed as necessary to counter cyber terrorism, the new law requires that telecommunications companies and internet service providers record every user's browser history for up to a year.

Yes, every website we've ever visited can potentially be accessed by government agencies, including the Department for Work & Pensions . More than this, the legislation actually permits hacking.

The police and security services can now access computers and mobile phones of citizens and companies to collate information – this means the Government has the ability to retrieve stored data and secretly download the contents of any phone or PC.

According to Jim Killock, director of the Open Rights Group , the Investigatory Powers Act is the "most extreme surveillance law ever passed in a democracy".

As a general rule, UK citizens are incredibly relaxed on privacy issues.

Beware the data trail

As I've written before, 60% of the population uses Facebook, which has a treasure trove of both fixed and changeable knowledge. Name, age, date, marital status, places

visited, places lived – the “like” button can track internet activity beyond the pages of Facebook itself.

As the MIT Technology Review states , in a global sense Facebook has collected the most extensive data set ever assembled on human social behaviour.

Then there are store loyalty cards. Great for the customer because we can receive benefits through repeated use – but on the other hand retailers can easily build up demographic profiles of customers based on what they buy, where and how often.

Payment by credit or debit card also allows stores to monitor purchase patterns of individual cards even if the identity of the user is protected.

The point is that all of this is connected and the vast majority of us have data trails cataloguing the minutiae of our daily lives.

And, as I write this, the National Crime Agency and National Cyber Security Centre warn that smartphones, watches, televisions and fitness trackers could be used by cyber criminals to hold people to ransom over personal data...

Technology is a wonderful thing and I’ve got nothing to hide (I think) – but I sometimes wish we could all go back to wind-up watches, analogue TVs, pen and paper, books, landlines and the newspaper as main source of information.

My childhood, basically.

*** Dr John Jewell is director of undergraduate studies at Cardiff University’s School of Journalism, Media and Cultural Studies .**

Read more from Dr Jewell: Sky takeover would bring more power and influence to Murdochs