The day of regulating looms

***David Birch**. is worried about digital security as more and more devices are connected to the internet. He believes the only solution is the regulation of the infrastructure*

A certain pop star had a husband who was, as is so often the case, getting on too well with the nanny. He recorded some of his below-stairs adventures on his iPhone, no doubt to act as a comfort in his later years. Unfortunately, he had either forgotten about iCloud or could not work out how to configure it correctly. The screen saver on his wife's iPad was transformed from a selection of treasured family snapshots into a cross between a post-modern fiesta and a flick-book version of activities that would surely unite most of the world's religions in horrified awe.

Interconnection has increasingly unexpected consequences. A generation on from the famous "on the internet, nobody knows you're a dog" cartoon, the situation is much more perplexing. On the internet now, nobody knows you are a fridge, or, for that matter, a dog pretending to be a fridge. Indeed, after last October's massive internet outage caused by a "botnet", many commentators remarked how odd it was that a network designed to withstand nuclear war could be disrupted so badly by toasters.

This does not look good. We have gone mad connecting up things but have overlooked how to disconnect them. Or, to paraphrase: doors are easy, locks are hard. Anyone can connect their kettle, car or children to the internet, and it is tempting to do it just because it can be done. But keeping them secure? That is another, and altogether more difficult, problem. If we are going to make an Internet of Things safe for financial services of the future, if we have a vision of luggage that can sort out least-cost routing or cars that can buy their own insurance, then we are going to have to pause for breath and rethink the platform, because that botnet is only the beginning.

A botnet is a collection of devices (computers, toasters, cameras and anything else that can be reached through the interweb tubes) that has fallen under the control of some third party. It can then be used in a massed and concerted fashion either for good (eg searching for radio signals that might indicate extraterrestrial life) or evil (eg overloading bank websites so that customers cannot get through). The botnet mentioned above is a work of art. It wanders the highways and byways of the internet looking for devices that have been connected but do not have security defences in place. This turns out to be almost all of them. Either the password has been set to "password", there is no password, or there is a bug in the software than can be exploited.

This last category is especially vexing. Suppose it turns out that my smart toilet (these do exist by the way – I have photographic evidence) has been shipped from South Korea with an old version of software that the hackers can easily exploit. Now my toilet is going to need patching and then upgrading. But supposing the facilities to patch and upgrade my toilet do exist ("do not flush, upgrade in progress, download complete in 22 minutes"), how will the manufacturers persuade me to do this? What if they have gone out of business? What if the upgrade is itself a trick designed to subvert my toilet for the amusement or profit of eastern European hackers? My head hurts.

> “We cannot trust the populace to configure their devices

The truth is that just as we need a digital identity infrastructure for people, we also need a digital identity infrastructure for things. But, as Bruce Schneier, the noted security expert, rather eloquently said, the thingternet's market failure is a kind of post-industrial pollution. It is an externality that can only be fixed by society and, as unfashionable as that might be, that means regulation. Before it is too late.

If we do not get on with it, you will be stunned by just how dull the war movies of the future will be. No more *Saving Private Ryan* or *Starship Troopers*: the infantryman of the next global conflict will be in his underpants, eating tuna out of the can and staring at a bank of flickering screens, not storming a beach. I have no idea how we are going to defend against their massed ranks, but I think it may have something to do with the regulation of infrastructure. We cannot trust the populace to configure their devices any more than we can we trust pop stars to do so. This means that selling phones that can hacked, even if it is by the CIA, ought to become as unthinkable as selling cars without seatbelts. ■

***David G W Birch** is a director of the secure electronic transactions consultancy, Consult Hyperion, and a visiting lecturer at the University of Surrey. He is an internationally recognised thought leader in digital identity and digital money, one of Wired magazine's top 15 global sources of business information and a research fellow at the CSFI*