



## VNUNet – Security: Is Technology Saint or Sinner?

By Clive Longbottom, Service Director, Quocirca Ltd

The latest problem to be thrown at us, on top of war, global warming, disease etc, is that we are 'sleepwalking into a surveillance society'.

The worry is that, owing to all the data being collected these days, we no longer have any real privacy.

We are covered by cameras, the 'powers that be' have oodles of information on everyone of us, and the private sector has got in on the act with the likes of loyalty cards.

Yet, the vocal groups (and who knows if these are the minority or the majority) want it all ways.

They want their privacy, while trying to make sure that all these Johnny Foreigners don't come over uninvited, that the 'man next door' doesn't claim sickness benefit while on a mountaineering holiday in Tibet and that when needed, the emergency services will have everything at their fingertips to know exactly what drugs can and can't be given to you while you're lying in the road, and/or have access to high-definition CCTV footage to identify who it was who kicked seven shades of the proverbial out of you.

I think that we need to look at pragmatism and try to put 'privacy' into context. What do we mean by privacy here?

Do we really think that all of the 13 million CCTV cameras in the UK are being watched by forces which are just waiting for us to inadvertently drop a paper hankie on the street?

Do we really believe that hordes of people are sitting in some dusty basement in Cheltenham reading the email that you sent with that particularly non-PC joke in it?

Are we worried that we might just get caught after we've mugged some poor unfortunate?

Could this be it? We're not really bothered about 'privacy' as such, but we're worried that we might get caught? Speed cameras would seem to be a prime example of this 'privacy' argument.

There are many groups and individuals whose worries are more pragmatic: the security, integrity and

accuracy of the information being held on us. This has less to do with privacy, and more to do with reality.

For example, if I'm the person lying in the middle of the road, I do want the paramedics, police and fire brigade to know that I am allergic to penicillin, that I have epilepsy, and that I am already on a collection of prescription drugs for a range of problems.

This knowledge could save my life and, as I am a simple soul, I don't care who knows all of this. Now, let's say that I was the chief executive of a major company that is just going through a sensitive acquisition.

My medical records could say that I have only a few months to live. This is very important for the medical profession to know, but probably not what I'd want splashed over the financial pages of the papers.

There's also the problem of what the 'powers that be' will do with information. All we have to do is look at the likes of Hoover, Beria, Trotsky and Hitler as to what can happen when too much information is given to someone who is a little on the unstable side.

But, the majority of these despots did their dirty work without technology. So is it technology that is to blame? Yes, technology means that we can gather and analyse a lot more information.

Yes, technology means that people thousands of miles away are just like the risks of having cleaners in the office 50 years ago: if you don't take careful steps, you're leaving everything available to them. Yes, the black hats (bad hackers) are cleverer than ever and there are relatively more of them.

But does this mean that we should ban any database of information held on us? Does it mean that all information should be kept in isolation from other information?

If we continue in this way, we'll see more headlines where a child dies owing to information from one group not being available to another, to people who should be being tracked being lost due to insufficient data being available, to the continued billions of pounds being wasted in fraudulent claiming of benefits, of insurance claims, the booming black market economy and so on.



ID theft will continue to rise without any means of being able to prove irrevocably who we are, and that ID can be taken from us.

And for anyone who has had full ID theft occasioned against them, then all of a sudden, you really wish that you'd backed the implementation of ID cards, at least in a correct way.

(Please note that I am not backing the government's half-hearted, half-baked way of providing government-backed false IDs.)

To my mind, it's technology which can help us by ensuring sophisticated controls over access to data. We can design, say, a DNA database that is just that: a genetic fingerprint that is held against an identifier.

We could do the same for iris recognition and/or fingerprinting. Three different databases, none of which actually provides any information against named people.

To get onto these databases, you have to go through three different groups. Why? So that any chance of using insiders to create false IDs is minimised.

Any check against these databases would use full auditing. Any access to any field within the database is time stamped and stamped with an access code showing which user or body nominally accessed that field.

Security profiles then begin to take over; having verified that the DNA, iris and/or fingerprint are in each of the databases, what else do we need to do?

Do we need to be able to carry out another match to ensure that this person is who they are saying they are? Maybe a PIN or something similar? OK, a fourth database, maybe within the private sector.

Again, all that this has is the PIN against a unique identifier. We now have up to four pieces of unique data against four unique identifiers. In comes database number five: a correlation database of unique identifiers.

If all of these unique identifiers correlate as being from the same person, we can pretty much assume that we have a match. And at no stage have we had to go to a database that has any names or other personally identifiable information held within it.

However, if this is the police, ambulance or fire brigade, they may then need to go to a different database where such personal information is held.

Again, all fully audited against access type, named ID and, where necessary, correlated against biometric information of the accessing individual.

For the highest levels of information being held on us, we need the same sort of approach that we have for nuclear warheads being set off: a dual key system.

No single person should be able to access every last item about another without some balance being available.

For me, we have to look at data pragmatism. I want to be able to walk the streets without too much fear of aggravated assault against me, I want to be able to see my insurance premiums go down because thieves find it harder to get away with misdemeanors, I'd like to see my tax go down due to fraud being eradicated.

This won't happen unless we make the most of technology, but also use appropriate technology as the controls against inappropriate usage.

## About Quocirca

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

## Quocirca Services

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca also provides bespoke primary research services through its daughter company QNB Intelligence. This involves interviewing thousands of senior decision makers on a quarterly basis.