KCS Group Europe

Biometrics: The Eyes Have It?

10/01/2018

How much is your life worth? Possessions might easily amount to a few thousand pounds. A house, many thousands more. The cost of raising, educating and such push up the value of 'you' even higher. Plus, of course, most people tend to view their life as somewhat priceless.

For scammers, the answer is £5.82.

The world of data security and leaks was once again broadened last week, when it became apparent that the personal information of over one billion Indian citizens had been breached and was for sale on the Dark Web and through WhatsApp for 500 rupees (£5.82). While officials have (as usual) been quick to condemn the reports and claim that nothing can be done with the misappropriated data, it is difficult to find comfort in this when the haul could include thumbprints, retinal scans and personally identifying information of each individual – information that is for obvious reasons impossible to replace – and when there already exists the capability to use this information to fake 'Aadhaar' cards, which are used to buy staples such as food and various government services.

In India then, there is the very real possibility that the component parts of one's official identity could be compromised, and used either by bad actors to illegally claim the benefits or to blackmail the original owner for their return. (This presents more difficulties than it otherwise might – you might be able to change your password or set up a new bank card, but very few of us can switch out a set of irises or fingerprints).

There is nothing inherently new in this – 'fake IDs' have after all been around for centuries and database compromises before have offered personally identifying information which is manna for hackers. The problem here though is twofold. Firstly, the sheer scale – with over a billion-people logged in the Aadhaar database this could lay claim to being one of the biggest breaches ever. Secondly, the degree to which the range of database information – from address to retinal scan – which might now be in the hands of criminals seems to be looming as the 'new normal'. Almost all of us have some level of personal information retrievable online and appear in various forms on various databases. As the digital revolution and the security-conscious state proceed apace, it is not beyond comprehension that databases such as Aadhaar could become commonplace – and all breached in the same way.

KCS Group Europe

Biometrics: The Eyes Have It?

ID theft is, on argument, even more of a long-term threat than ransomware or brute-force hacking. It may be possible to recover money and data, or put in place measures to prevent the damage should this occur. With things like fake ID cards and biometrics, not only could criminals cause long-term damage, but they might even do it without your knowledge, until such a time when your inability to 'prove who you are' is exposed – by which time it is too late. Should any of the Aadhaar entrants find themselves unable to get food supplies this week as a consequence of their impersonators having gotten there before them – or through attempting to ransom the data back – this will be Aadhaar's responsibility for a failure of proper defence.

In the wider scope, if biometrics are the future, then the consequences for data will be severe. Leaving aside the question of whether mass biometrics are actually fundamentally necessary, the challenge they present to database security managers is severe. It goes without saying that the more tempting the fruit, the greater the attempts will be to try and pluck it, and with a clear capability among the criminal fraternity to enact data loss on a massive scale a compromise would be expected rather than anticipated. And with such important data, this is definitely not good enough.

Of course, the consequences for GDPR would be immense. If one extends data loss to our eyes and our fingerprints, as may happen, even the biggest fine levied for compromise of statistical data would be seen as minute in comparison.