

## Cambridge Over Troubled Waters

---

26/03/2018

**The Cambridge Analytica saga has confirmed, as if further evidence was needed, that your data is less secure than ever. Whether there was genuine loss of oversight or deliberate malfeasance, the hard truth is that millions of people – and billions of relationships – were used illicitly, and that this is not likely to be the first or last time that data is on the line.**



The 'personality test' used allegedly by Dr Kogan is not even new. These sorts of innocent quizzes have been doing the rounds on Facebook and LinkedIn for years, offering you the chance to find answers ranging from your personality type to your Force alignment. Sometimes they are for something approaching a genuine experiment, sometimes they are used as entrées to a scam (hey, Sith happens). But in every case, the data of the user – be it entries actually used in the tests (ie name, personal qualities, preferred Kogan crystal colour) or data that is harvested consequentially (everything else) would be transferred back to the originator of the test program – and after all, that person could be anyone. In any case there is a question of transmitting significant quantities of personal data to, effectively, an unknown party.

The difference this time was that the Kogan test did not only take user data, but the data of all people connected to that user. So, with a sample size of just over a quarter million people taking the test, we end up with data of fifty million, based upon relationships, connections, likes, and any other sorts of interactions. The scope of data is thus broadened to essentially encompass anything able to be gleaned from these individuals' profiles – a staggering amount with equally broad consequences.

In this case, all of the data on both the respondents and their connections was used to build psychological profiles and predictions as to voting patterns, and then attempt to sway them accordingly. Quite aside from the strict legal implication of whether this was election tampering through unauthorised access to and use of data, the general trend remains that data can be, and is, being obtained and put to use without the consent of anyone involved. In this instance, the aim was to influence voters, but the data could be used for out rightly criminal process in itself. Bad actors might use it to socially engineer a target and then hit them with a specifically designed virus. Harvesters might simply collect the information as data for data's sake and throw it up onto the dark web.

## Cambridge Over Troubled Waters

---

Whether for electoral purposes or just plain criminal ones, we are giving our data away to people and purposes we know nothing of – when we know we are giving it away at all. As the Kogan case shows, sometimes we are never meant to find out.

The corollary to this is a simple one: why is it necessary to offer up this data in the first place, when we cannot ever be sure anymore where it goes and by whom it is seen?

Some may feel that it is vital that they take a free online personality test rather than follow more scientific avenues, and certainly there is a compulsion to ‘share’ almost every aspect of our lives, but in light of this latest incident – plus the patchwork of previous and similar instances down the years – it should be asked whether sharing and gratification takes precedence over personal security and doing whatever we can, however limited, to ringfence ourselves against bad actors. The threat is real and is being conducted on a scale which is still only now becoming clear. Is massive data loss worth such blind faith in presumed security? Answers to that could fill a whole personality test on their own...

### KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

**To find out more or to arrange a meeting to discuss your business needs, please...  
email the team at [info@kcsgroup.com](mailto:info@kcsgroup.com) or call (00 44) 2072451191**

---