CYBER BITES/ CYBER ESPIONAGE

It's Good To Talk – But Is It Safe?

The social messaging app, ToTok, ranked as one of the top free apps in the UK, Sweden, USA, India, and Saudi Arabia last year, has been found by the New York Times, (NYT), to be a spying tool for the United Arab Emirates ('UAE") government. The app has been downloaded millions of times from Apple and Google app stores. Both were concerned enough by the NYT allegations to remove ToTok in December 2019, but since 3 January 2020 Google has quietly reinstated it in Google Play Store.

The issue with the app is a devastatingly simple one– what happens to users' data once held on ToTok servers? The NYT tells us the data is harvested and then channelled by intelligence analysts into the UAE government. The app's publisher, Breej Holding, is, according to NYT, connected to DarkMatter, the notorious Emirati intelligence company currently under FBI investigation for cybercrimes, and with close ties to the UAE Government.

It is unknown how many people have used ToTok in the UK, or across Europe, or indeed how many UK/European companies have used the free app for conference calls. But the potential data breaches are profound if the allegations are true.

What are UK/European consumers to conclude from Google's decision to re-instate ToTok in its Play Store as of 3 January 2020?

How have Google complied with the GDPR duties they owe to all their customers by allowing an app which has the potential effect of spying on them? What re-assurance can Google give to its customers that ToTok is a safe app to use?

Google's decision to re-instate ToTok is at best opaque, and at worst may give rise to a class action lawsuit as far as their UK customers are concerned.

Serious UN data breaches – when were we going to find out?

Thanks to a leaked report, we learnt on Thursday that the UN offices in Vienna and Geneva were the victims of a cyber espionage attack in July 2019.

The attack bears the hallmarks of a sophisticated campaign very likely conducted by nation state hackers. From the leaked report we learnt that 42 servers were compromised, including those of the UN human rights and human resources offices. It is estimated a total of 400GB of data was downloaded during the attack. When confronted with the leak, the spokesman for

the UN Secretary-General, Stéphane Dujarric, described the cyber attack as ***"not a landmark event."***

The UN's decision not to disclose the data breaches raises a fundamental question: should public bodies protected by diplomatic immunity be absolved from scrutiny and accountability when it comes to data breaches of this nature?

The UN's decision flies in the face of the EU's own policy of *coordinated vulnerability disclosure* – a policy that requires every EU member state to disclose in a coordinated and responsible fashion breaches of their systems so that they can learn from each other.

We live in an age where vulnerabilities in computer systems, once discovered, are leaked by criminals with potentially geopolitical motives; and when certain governments are harvesting those vulnerabilities to develop offensive cyber-weapons themselves. The attack on the UN fits this profile. Why was the UN human rights office targeted? Could it be because it contains the most sensitive data that rogue states would love to get their hands on?

By deciding not to disclose, the UN has arguably behaved like an authoritarian state, damaging the reputation it has enjoyed and the very ideals it represents. This cannot be done in an accountability vacuum. Transparent decision-making processes are now needed in order to preserve the rule of law online and to hold government/world bodies accountable.

Although not under a legal obligation to disclose under the GDPR, the UN should not be allowed to hide behind its diplomatic immunity. It should be held accountable to the very people it is entrusted to protect and represent.