Thursday Thoughts – 1st July 2021

This week's Thursday thoughts has details of Android Apps which have been stealing users Facebook logins. I have a list of the apps concerned and some guidance on how to avoid this type of App in the future. Also this week news that the cloud-based IT management and remote monitoring solution for MSPs firm "Kaseya" suffered a ransomware attack. For those that use this product the company has released a "Compromise Detection Tool" which customers are being urged to download.

The ICO Annual Report has been published. This marks the end of the tenure of Elizabeth Denham and sets out what the ICO has being doing during the COVID-19 pandemic. An analysis of how well it has done this will be covered in a separate report to parliament, which should be publish over the summer. Also just published is by the Jersey Information Commission is a useful GDPR Jargon Buster (I've shared the links). The ICO issued it's first fine this year for a GDPR breach (all the previous ones have been for infringements of PECR). Mermaids Charity were fined £25,000 for failing to keep the personal data of its users secure after sensitive data was found to have been available for all to view online for 3 years.

Rather against the usual run of things the EU Parliament has approved the mass surveillance of private communications. It is now possible for all personal messages (email and messaging services) to be automatically searched "suspect content" by the service provider. Any suspect communications can be forwarded to the police.

In the US the Greenlight App used by millions of parents to pay allowances to children has been collecting a huge amount of data about it's users (children) which it reserves the right to share with a number of other parties.

This week's sole blog of the week is RMGirl's "What the FLoCs". No I didn't know what one of those was till I read the blog!

Blogs/Podcasts of the Week
Emily Overton - What the FLoCs

Android Apps Caught Stealing Users' Facebook Passwords

Google has removed 9 Android apps from Play Store. The apps (a mixture of photo-editing, optimizer, fitness, and astrology programs), some of which had been installed on over 5 million devices, tricked victims into logging into Facebook and then stole their log in credentials. The offending apps are: PIP Photo, Processing Photo, Rubbish Cleaner, Horoscope Daily, Inwell Fitness App, Lock Keep, Lockit Master, Horoscope Pi and App Lock Manager. In order to combat fraudulent developer accounts Google will now require developer accounts to use 2-Step Verification, provide an address, and verify their contact details. We can help ourselves by installing apps from known and trusted developers and keeping an eye on what permissions are requested by the apps that we install.

Kaseya Ransomware Attack

Kaseya, a cloud-based IT management and remote monitoring solution for managed service providers (MSPs) suffered a ransomware attack that triggered an infection chain which compromised at least 1000 businesses in 17 countries last week. The attack is being linked to the Russia-linked REvil cybercrime gang who are asking for a $70 million ransom payment. Which will apparently mean they will "publish a universal decryptor" that will unlock the affected systems. The US CISA issued an advisory, urging customers to download the Kaseya Compromise Detection Tool, enable multi-factor authentication, limit communication with RMM capabilities, and place RMM administrative interfaces behind firewall or VPN.

Greenlight App Collects A Huge Amount of Data about Children

The Greenlight App in the US is portrayed as "a financial literacy tool". The app allows parents to pay pocket money/allowances, choose the stores a connected debit card works at, set spending limits, and receive instant notifications whenever a purchase is made. However, there is a darker side as the company collects a lot of sensitive data about it's users (children) and reserves the right to share that information with other agencies such as "ad and marketing vendors," "insurance companies" and "collection agencies. The data includes names, GPS location history, purchase history as well as birth dates, email addresses and behavioural profiles. It collects the data so that it can deliver "tailored content" advertisements – not something youth privacy and education experts advocate for children as it is often manipulative.

ICO Annual Report 2020/2021

Elizabeth Denham has published her fifth and final annual report as the UK's Information Commissioner. During the entirety of the report the ICO staff were working remotely. Also in the response to the COVID-19 pandemic the ICO has been at the centre many of the key issues, including ensuring that data protection considerations were built into contact tracing solutions and emphasising the value of transparency and documentation of government decision making. You can read the report here: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf

EU Parliament Approves Mass Surveillance Of Private Communications

On the 6th July the European Parliament approved an ePrivacy Derogation which will allow "providers of e-mail and messaging services to automatically search all personal messages for presumed suspect content and report suspected cases to the police". This is being hailed as the end of privacy in digital correspondence and an enabler for automated mass surveillance. It will mean in all probability that criminals will move to another more secure platform or take their activities underground to other environments where these tools don't exist.

Jersey Information Commissioner produces a Jargon Buster/Glossary

If you don't know what "Personal Information" is or what you will find in a Data Protection Impact Assessment you will find the Jersey Information Commissioner has just produced a Jargon Buster/Glossary. Here is the link for those who need it:
https://jerseyoic.org/media/bl2g3e4p/29_tk_jargon-buster.pdf

Fines

UK ICO fines Mermaids Charity £25,000

Mermaids Charity has been fined £25,000 for failing to keep the personal data of its users secure after it set up an internal email group with weak security settings which allowed 780 pages of confidential emails to be viewed online over a period of 3 years. The ICO considers that Mermaids should have applied restricted access to its email group and could have considered pseudonymisation or encryption to add an extra layer of protection.

Blog of the Week

Emily Overton - What the FLoCs

Emily's blog looks at what Google plan to replace cookies with – FloCs. FLoCs are in essence tech replacements for third party cookies. They aggregate anonymous users with similar interests, collected through things such as our website and page visits and then send us "stuff" based on what we've looked at. We will still need to be permission for FLoCs to access our data but given that so few of us actually turn down consent on cookies let alone read the privacy and cookie notices that go with them I wonder how many will actually decline FLoCs when they see them . You will find the Blog here:
https://rmgirl.co.uk/2021/06/28/what-the-flocs/