Thursday Thoughts – 15th July 2021

There is lots to cover in this week's Thursday thoughts.

The most topical is should it still be possible to have an anonymous social media account, do we expect social media companies and ISPs to investigate and remove these accounts and what can we do as individuals if we see something troubling. There has also been an increase in stalking incidents over the last year, some rogue Facebook staff have been caught using their access privileges to do just that.

The EDPB has issued guidance on the roles of the Data Controller and Data Processor, and has included a discussion on Joint Controllers and many case studies to explain their guidance. This will be of great help to those struggling to understand their role. I've included an "In the news" section this week which includes; criminals behind a banking trojan scam being arrested in Spain; an example of where AI was used to fire an employee and why two houses were searched after the data processor reported the "Matt Handcock" CCTV data breach. Finally in the news there is some interesting research on whether a smart doorbell makes your home more attractive to burglars.

Also this week there are the usual threats and warnings and quite a raft of fines for a variety of infringements of GDPR.

Blogs/Vlogs of the Week
Richard Merrygold - How to deal with GDPR related customer complaints
Debbie Reynolds - The frailty of consent
Emma Day - The education data governance vacuum

Anonymous Social Media Accounts

There is lots in the media this week about whether it is still appropriate for people to have an anonymous social media account. With hate crime on the increase and a number of anonymous accounts being used to spread the vitriol. It is not surprising that many have signed a petition to enforce the use of formal identification when setting up a social media account. There are however many good reasons why a person would want to remain anonymous not least victims of domestic abuse or stalking, whistle-blowers or those transitioning to a new gender. The social media companies (especially LinkedIn, Twitter and Facebook) and ISPs can definitely do more. They should take an active role in investigating and removing accounts inciting hatred. But we all have a role to play in stamping this out. If we see something that should be reported and it is safe to do so we should. Each platform gives us a way to do this (links below):

https://help.twitter.com/en/safety-and-security#sensitive-content
https://www.facebook.com/help/181495968648557/
https://support.tiktok.com/en/safety-hc/report-a-problem
https://help.instagram.com/contact/383679321740945

https://www.linkedin.com/help/linkedin/answer/37822

Facebook Engineers Used Access Privileges to Stalk Victims

It is widely reported that there has been in increase in stalking incidents over the last year. This week Facebook hit the news with the publication of a new book that exposes insider threats at Facebook. One such threat is the story of how Facebook staff used their access privileges to do just that. In one instance a Facebook staffer accessed a former date's location after she stopped responding to his texts and in another a victim was tracked to her hotel after having a fight during a date.

EDPB Produces Guidance on the Roles of Controller and Processor

The European Data Protection Board has finally issued it's guidance "on the concepts of controller and processor" under GDPR. This includes much needed comment on joint controllership which we will see explained over the forthcoming weeks as the data protection experts get to grips with the text. There are also many helpful examples in the ruling including ones for healthcare, payroll and head-hunters. You will find the source document here: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

News

Cybercriminals Behind Banking Trojan Arrested in Spain

16 individuals were arrested in Spain in connection with two banking trojans (Mekotio and Grandoreiro). The individuals were involved in a social engineering campaign that targeted European financial institutions whereby email spoofing was used to divert large amounts of money to their organisation's accounts. €87,000 of the €276,470 transferred has been successfully recovered.

AI used to Fire Employee

An Amazon employee in the USA was fired by an automated email. The 63-year-old Army veteran who had been employed by Amazon for 4 years was sent the email because the algorithms Amazon used to track him (and other staff) had decided he wasn't doing his job properly.

Two Houses Searched and Data Processor Reports CCTV Data Breach

The Matt Hancock saga continues. Unusually the Data Processor rather than the Data Controller has reported the CCTV data breach. The ICO said in a statement: 'EMCOR Group (UK) plc, which provides facilities management and CCTV services for the Department of Health and Social Care (DHSC), has submitted a breach report as a processor of personal data, alleging images were taken from the DHSC CCTV system without consent from either EMCOR Group (UK) plc or the DHSC. ICO teams then searched two residential properties in the south of England and seized electronic devices as part of their investigation into how the material emerged.

Does A Smart Doorbell Make Your Home More Attractive To Burglars

Researchers from Cranfield University have said that “installing a smart doorbell on your abode may actually increase your home's attractiveness to burglars”. The findings conflict with the marketing message of video-enabled doorbell companies. Dr Duncan Hodges believes that residential burglary rates are "unlikely" to be affected by the presence of a smart doorbell arguing in fact that the opposite is true because the devices are noticeable they may be used by experienced burglars to identify a properties that has “potentially more high-value items".

Fines

Luxembourg - Logistics Company Fined €15000

The DPA in Luxembourg fined a logistics company €15,000 for failing allow its DPO to exercise their role. The organisation had failed to invite their DPO to all relevant meetings and neither had it allowed the DPO report directly to the highest level of management.

Denmark - Medicals Nordic Fined €80,700

The Danish DPA has fined Medicals Nordic €80,700 for using WhatsApp to transmit confidential health data. All employees of a test centre were invited to a work WhatsApp group which was used to share confidential information with the company's central administration. There were no checks to ensure that only those who needed the information had access to the chat.

Croatia - Administrative Fine On An Insurance Company

The Croatian DPA has imposed an administrative fine on an insurance company based in Zagreb. The business concerned was subject to video surveillance but had failed to provide notice that surveillance was taking place.

Spain - Malagatrom S.L.U Fined €4000

The Spanish DPA has fined Malagatrom S.L.U €4,000 on for publishing the personal data of a person who made a complaint on Amazon. The details included on the Amazon store page of the defendant company included the complainant’s first and last name, address, phone number as well as the name of his wife and her mobile number.

Spain - Caixabank Fined €50000

The Spanish DPA fined Caixabank S.A. €50000 for continuing to send advertising to a data subject even though he had objected to the processing of his data for advertising purposes.

€450,000 fine for UWV from the Dutch DPA

The Dutch DPA fined UWV € 450,000 for failing to secure group messages via the 'My Workbook'. Personal data including health information of 15,000 individuals was breached.

Italian DPA fines dentist €20,000

The Italian DPA fined a dentist €20,000 after the dentist refused to treat a patient who has disclosed their HIV status.

Threats and Warnings

Microsoft Patches 117 Vulnerabilities

This week's July Patch Tuesday updates from Microsoft fixes 117 vulnerabilities in Windows, Bing, Dynamics, Exchange Server, Office, Scripting Engine, Windows DNS, and Visual Studio Code.

Latest Trick to Get you to Download Malware

The cybercriminal's latest trick which involves sending out a non-malicious office document which has code in it to disable macro security warnings. The code then allows malware to be downloaded onto the victims' machine.

Vlogs of the Week

Richard Merrygold - How to deal with GDPR related customer complaints

Richard's latest data protection diaries video stresses the need to look at GDPR complaints dispassionately. It is really important to take the "personal" out of the equation when dealing with customer complaints, especially those dealing with GDPR which often quote from legislation, guidance and are often written with the assistance of a template. For a small business this can be very frightening. The key is to look at the issue(s) that have been identified, investigate any shortcomings and address any issues then share the facts with the complainant. You can watch the vlog here: https://www.youtube.com/watch?v=MQNOhzUPZtY

Debbie Reynolds "- The frailty of consent

Many companies are now asking for consent to data sharing little by little over a period of time rather than asking for consent for more data at the outset. This Vlog by Debbie explains the reasons why businesses will try to gather lots of small consents because these "may eventually culminate in consent for larger data sharing" and then discusses the frailty of consent including and the move whereby third parties are now obtaining consent from data subjects rather than obtaining their data through a "vendor". Incremental consent is going to require a lot more monitoring by the data subject to ensure their data does not get into the wrong hands. Companies requesting data need to be much clearer about who they will be sharing it with and what they plans to use it for. You can listen to the Vlog here: https://www.youtube.com/watch?v=dEcCS_LLkiE

Emma Day - The education data governance vacuum

This blog shines the light on the work being done to bring in a child rights-based approach to education data. So much data is collected in the education setting and yet children have little choice over what apps and platforms they use. With the EdTech sector estimated to be worth £3.4 billion in the UK there is a lack of governance within the sector. You can read the blog here: https://digitalfuturescommission.org.uk/blog/the-education-data-governance-vacuum-why-it-matters-and-what-to-do-about-it/