Thursday Thoughts – 18th February 2021

Last week's Thursday Thoughts attracted quite a bit of debate especially on the topic of Clubhouse. This week there has been more conversation in the media about whether there are some people who definitely should not be on it (MPs, particularly when you think about who may be in their mobile address book). There was a follow up meeting of the Handforth Parish Council which was "public" and the full transcript and Zoom has made its way into the media (you may be interested in Jenny's Blog for insight on this).

This week I have also seen a number of companies being approached by the ICO to see why they have not registered as Data Controllers even though it is obvious (often because of the number of staff they have and turnover) that they are. If this has happened to you then I can help guide you through the process. In the news this week Apple iOS 14, Poor Password Security, ICO policies released, using add ons like Grammarly, Facebook's "oversight board" make their first ruling and dark web drug sales and much much more!

Blogs and Videos of the Week
Jenny Barnes - Zooming through Handforth
NCSC Small Business Guide: Cyber Security.
Merry Marwig 2021 Trends in Combating Deepfake Impersonation Attacks
Gabriel Freelander – You Can't Send this Here

A Reminder to update your policies.

The UK GDPR is the UK General Data Protection Regulation and is a UK law which came into effect on 01 January 2021 to write the GDPR into UK law. It forms part 2 of the Data Protection Act 2018 and all the articles and recitals are numbered the same as EU GDPR. All references to the GDPR in your policies should now be turned into references to the UK GDPR. What this means is that you need to add a note to that effect in your all your data protection and privacy documentation. In practice whether you change every reference to say UK GDPR or add a footnote to each document to say "All references to the GDPR should be read as references to the equivalent provision in the UK GDPR" it is up to you.

Remember though you may need to comply with both the UK GDPR and the EU GDPR if you operate in Europe, offer goods or services to individuals in Europe, or monitor the behaviour of individuals in Europe. You may need to take legal advice on what your EU obligations are and any overseas data collected before 01 January 2021 will still be subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR').

Clubhouse or Don't – It's Up to You

Many are happy to use a platform like Clubhouse because of the utility it provides. Considering the information it collects about them as a necessary "hoop to jump through" in order to be able to use the platform, and trusting that any glitches will be ironed out. These individuals will likely also embrace the "Single Sign On" feature because it helps them. That's fine it's your choice. Just

remember that Clubhouse takes all your content and account information from every site you link to it, adds that to what you create and share on their platform, who you messaged and then tracks all people, accounts, and groups you are connected to and how you interact with them.

If you work in a sector such as defence, government, healthcare, or politics (to name a few) I would think very long and hard about whether you should be on Clubhouse. Just because you can doesn't mean you should. If you think you should be on Clubhouse then clear out your contacts list or use a different phone to the one that has all your clients and friends on it. You will also want to be aware that recordings are taken while the app is live. Most importantly for these individuals you need to understand that in order to "invite" friends onto the platform Clubhouse REQUIRES that you to share your address book. There may be numbers in your address book that you would not want to know that you are on Clubhouse, or indeed there may numbers that you have because of your privileged position (would they be happy with their number being shared).

Poor Password Security

The recent "Water Treatment Facility Hack" was because of poor "Password Security" according to the Hacker News. The threat actors managed to access the supervisory control and data acquisition (SCADA) system via TeamViewer. Which had been installed on one of the plant's several computers that were connected to the control system. **The computers in question were running 32-bit versions of the Windows 7 operating system, shared the same password for remote access and were exposed directly to the Internet without a firewall.** Unsurprisingly the state officials have recommended that utilities companies **"**Restrict all remote connections to SCADA systems" especially if they allow physical control and manipulation of devices, use "one-way unidirectional monitoring devices to monitor SCADA systems remotely" and then "Keep computers, devices, and applications, including industrial control systems software, patched and up-to-date, and use two-factor authentication with strong passwords." You can read the full report here: 2020.https://thehackernews.com/2021/02/poor-password-security-lead-to-recent.html

Password Advice

Did you know that you can password protect your Word, Excel and PowerPoint files. This is particularly helpful when sharing information that is confidential. Just remember to share the actual password via a different communication medium to the one you send the document on(phone, text face to face)!.

The NCSC has some great advice on what makes a good password. In this article about using 3 random words https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0.

Updates on UK Policy from the ICO

It has been a busy 12 months for the ICO here the policies that they have published since February 2020.

- January 2021. An updated BCR communication following the EU-UK Trade and Co-operation Agreement to the International transfers after the UK exit from the EU Implementation Period.
- December 2020. A new Data Sharing Code of Practice, alongside a data sharing information hub with further resources and support.
- December 2020. Guidance on sharing personal data with law enforcement authorities.

- December 2020. Guidance on data sharing and reuse of data by competent authorities for non-law enforcement purposes.
- November 2020. Guidance on criminal offence data.
- September 2020. Publication of the Accountability Framework, which provides detailed guidance on complying with the accountability principle.
- February 2020. Guidance on codes of conduct and certification.

News

Apple's iOS 14 contains its own "Fraudulent Website Warning"

Up until this point this feature relied on searching an "obscure Google database". Apple have decided to use it's own servers as a middleman between your phone and Google's databases to access the database. This is part of the new privacy feature in iOS 14. You can read more here: https://gizmodo.com/apples-keeping-googles-prying-eyes-out-of-ios-14-1846253965

Did you ask the IT Team if you could add that add-ons?

Most people won't think twice before installing "helper/productivity" add-ons, like Grammarly, online JSON converters or online Translation tools. The information that these tools capture is a form of data sharing. It stands to reason that it should be recognised and it's use mapped in your Record of Processing Activities. Using these tools without letting the IT team know could represent a compliance or security problem.

Data protection rules and M&A deals

Arnold Karanjain's article in Business Daily discusses how and why data protection and privacy safeguards have changed the M&A landscape. When GDPR came into force the area of the due diligence was impacted with potential buyers now required to consider data protection and privacy as part of their analysis. Some M&A transactions proceeded without proper due diligence with expensive repercussions (Marriot) but some 58% of planned M&A transactions stalled as a result of GDPR Compliance concerns. You can read Arnold's article here: https://www.businessdailyafrica.com/bd/opinion-analysis/ideas-debate/-data-protection-or-break-m-a-deals-3292406

Dark web drug distribution conspiracy

Two men have been charged for using a dark web marketplace and encrypted messaging service Wickr to sell pills. The pills in question looked like Adderall (a common ADHD medicine) but in reality contained highly addictive synthetic stimulant methamphetamine. You can read the more here: https://www.infosecurity-magazine.com/news/duo-multimilliondollar-dark-web/?utm_source=dlvr.it&utm_medium=linkedin

Facebook's Oversight board make their first ruling

Facebook's Oversight Board were set up at the instigation of Facebook for the "governance of the Internet". The committee issued its first six decisions on January 28, 2021 relating to the removal of content from the platform. This is a historical moment and a step in the direction of radically changing both the nature of the Internet and the relationship between platforms, states and public institutions.

New tools to check previous editions of Contractual Documents

France has launched a selection of tools which allow users to "explore the contractual documents of the main online service providers and compare their evolution through time". They have a database of the major online platforms' terms of services or privacy policies (including Facebook, Google, Amazon, Twitter, Netflix and Spotify). The tool is in both French and English and can be found here:
https://disinfo.quaidorsay.fr/en/open-terms-archive/scripta-manent?service=123Greetings&typeofdocument=Privacy+Policy

Secret Chat in Telegram Left Self-Destructing Files On Devices

If you use Telegram and haven't updated it from version 7.3 you should do. Telegram only end-to-end encrypts chats if users enable the "secret chat" feature. These secret chats can be made self-destructing. A bug that made it possible for threat actors to "access self-destructing audio and video messages after they disappeared from secret chats" has been patched in Version 7.4.

Videos and Blogs of the Week

NCSC Small Business Guide: Cyber Security.

This useful blog from the National Cyber security centre offering affordable, practical advice for small businesses on what to do about Cyber Security. It includes an explanation of the need for passwords and 2FA. The link is here:
https://www.ncsc.gov.uk/collection/small-business-guide/using-passwords-protect-your-data

Merry Marwig 2021 Trends in Combating Deepfake Impersonation Attacks

Merry predicts that this year "there will be a rise in cybersecurity companies getting into the deepfake-detection business to help industries combat this threat." We already experience email impersonation and phishing attacks targeting executives across the globe. This article about "Deepfakes"(videos or audio that is manipulated by AI). Shows that it is possible to produce content that can be compelling and difficult to detect. We are seeing increased incidents of criminals targeting executives and CEOs and using audio and video Deepfakes with their likeness to make staff act out the criminal's wishes. You can read the article here:
https://research.g2.com/insights/2021-trends/deepfake-impersonation-attacks-trends-2021

Jenny Barnes - Zooming through Handforth

Jenny speaks from experience having been a member of the now infamous Handforth Parish Council. Her reflection on the lessons she learned as a result are enlightening and a warning for anyone planning to go into local politics; expect hoodwinking from the start (or tactical scheming), be cautions when questioning because you can lose friends. She points out the system is out of date and needs reforming. So when you watch the 18 minutes of edited video or indeed this month's public Zoom in full you need to bear in mind the progress made in the last eight years. You can read Jenny's Blog here: https://www.ivity.org/post/bulliesout-you-have-no-authority-in-handforth

Gabriel Freelander – You Can't Send this Here

Gabriel shared one of his great videos this week. Most of us have seen an increase in the use of a number of different communication channels over the last 12months, it is no longer just email and text. We need to remember that just because someone messages you in a certain way it is not always appropriate to respond on the same platform so "don't make it a habit to just hit respond".

The important thing is to use the right communication channel for the message. You can see the video here: https://videos.wizer-training.com/videos/526587930b7c46558f67353cd67bec0d.