THURSDAY THOUGHTS

Today there was great news on the transfer of Data to Europe with news that an “adequacy” decision will be made well ahead of the June deadline. More positive news came that the world's largest illegal dark web marketplace has been “taken down”. There is news of the “New and Improved” New Zealand Privacy Act and a ruling by the European Court of Human Rights on the publication of tax evaders' data. 2021 has also seen the rise of day time TV “Data Breach Claim” advertisements – it appears this is the replacement for PPI claims!

This week the news has been full of the WhatsApp privacy terms and conditions debate. I have read many articles on the matter and listened to a number of “experts” and I include my considered thoughts on the matter as well as some helpful links to documents that may help you make up your own mind. Whether or not you decide that it is a step to far will really depend on your own situation and privacy preferences. If you haven’t already done so make sure your privacy settings are as tight as the platform allows. You can find help and guidance on this on the NCSC website.

Blogs of the Week
HR Dept - How Employers Can Help Working Parents Through School Closures
Altrincham HQ - How To Limit Your Sales & Marketing Distractions In The New Year

Brexit and Data Transfers

AKA the adequacy debate. Last week I outlined that there was a 6 month "window" permitting seamless data transfers between the EU and UK. Today there was great news that a "UK adequacy decision" is on its way. The Commission announced that it will finish it’s assessment and send it to the European Data Protection Board for opinion in the next few weeks. You can watch the EU Committee on Civil Liberties, Justice and Home Affairs discussion of this and other matters here: https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20210114-0900-COMMITTEE-LIBE_vd (watch from 10:45)

The World's Largest Illegal Dark Web Marketplace “Taken Down”

It was announced this week that DarkMarket had been shut down by Europol as part of an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the UK's National Crime Agency, and the US Federal Bureau of Investigation. DarkMarket was the world's largest online marketplace for illicit goods and was believed to have had 500,000 users and 2,400 vendors who carried out transactions to the value of €140 million in bitcoin and monero.

New Zealand Privacy Act 2020

The “new and amended” New Zealand Privacy Act came into effect in December 2020. The act applies to any website, company or organisation that collects, uses, shares or stores personal information from individuals inside New Zealand. Similar to EU GDPR, it governs the handling of personal data (according to 13 Privacy Principles); requiring you to notify and inform users about the collection, use and sharing of data and giving individuals the right to access and the chance to correct their data. You can read more here: https://www.cookiebot.com/en/new-zealand/

Are Data Breaches the Next PPI Claim?

According to the news this week … as the PPI claims window is slammed shut another [data breach claims] opens. This follows adverts from claims lawyers on daytime TV promoting data breach claims. If you receive correspondence from a lawyer making a claim following a "breach" make sure to get appropriate specialist advice. There have been examples recently which cite the law incorrectly or misrepresent its meaning.

Guidance

Ruling on Publishing Tax Evader Data

The European Court of Human Rights has made a ruling that the publication of tax evaders' data could be a violation of art. 8 of the Convention. This is because the tax evaders data includes the amount of tax arrears and debts, the evader's identification number, the evader's name and home address. Any presumed violation must be balanced with "the public's right to be informed".

Using Video Conferencing Services Securely

Many of us have been using video conferencing services, such as Zoom and Skype for a while now. However in the rush to home working did you set them up safely and securely. For example the latest Zoom update is 5.4.9. Advice on how to set up your video conferencing from the NCSC is: https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely

House of Lords Report on Artificial Inteligence

This week a report from the House of Lords has called for a minister-level committee to lead the country's efforts on AI. The report entitled "No room for complacency" includes a number of recommendations include the need for authorities to be given power to challenge unethical AI and the requirement to develop standards for ethical AI. The report is at: https://lnkd.in/eQYipV7

Should Cyber Training Include Phishing

One of the most common problems when it comes to cyber training of staff is how to protect the business against Phishing. Is it enough to give staff a presentation which shows an example of the latest scam out there or is there another way. Some organisations are choosing to go down the "phishing simulation" route because of the risk to their business. If you want to follow a discussion on phishing simulations, how to approach them, and their unintended consequences there is a great webinar here: https://www.wizer-training.com/webinars/phishing

The Benefits Of Adopting A Cloud-System

The NCSC has released a new white paper which explains the potential benefits of adopting a cloud-system. If you are considering a move to a cloud system and are concerned that it will result in more overall risk than traditional systems the paper will explain how to make a fair comparison and the security benefits such a move could deliver. Take the time to understand the cloud services available and you, a good service will make advanced security available to all customers. You will find the white paper here: https://www.ncsc.gov.uk/blog-post/the-elephant-in-the-data-centre

Patches and Bypasses

Google Security can be Bypassed using Google's Speech to Text API

The Google "Speech-to-Text API" can bypass the Google reCAPTCHA Security Plugin (with 97% Accuracy). You can read more here: https://thehackernews.com/2021/01/google-speech-to-text-api-can-help.html

Microsoft Patches

For the first patch Tuesday of 2021, Microsoft released security updates for Microsoft Windows, Edge browser, ChakraCore, Office and Microsoft Office Services, and Web Apps, Visual Studio, Microsoft Malware Protection Engine, .NET Core, ASP .NET, and Azure. The most severe issue is with Microsoft Defender (CVE-2021-1647). You can read more here: https://thehackernews.com/2021/01/microsoft-issues-patches-for-defender.html

Fines

Germany Fine Company €10.4 M For Video Monitoring

In Germany the State Commissioner for Data Protection of Lower Saxony fined notebooksbilliger.de AG €10.4M because they had been monitoring their employees using video cameras in workplaces, sales rooms, warehouses and common areas. The company had no legal reason for this although they claimed the cameras were to prevent crime and to track the flow of goods. The Commissioner considered that there were other systems that could be put in place, such as bag searches that could achieve the same aim.

British Airways

It is expected that the largest group claim over a data breach in UK legal history will be filed against British Airways this year. Over 16,000 customers have signed up to the action and victims could receive £2,000 each which would mean a total bill for BA of £800m.

Leaks and Cyber Attacks

Police Arrest 21 "WeLeakInfo" Customers Who Purchased Personal Data

21 people were arrested as part of a nationwide cyber crackdown. The individuals we former clients of WeLeakInfo[.]com an online service that had been selling access to data hacked from other websites. The UK National Crime Agency said suspects had gone on to commit further offences using stolen personal credentials. Those arrested were detained on suspicion of Computer Misuse Act or Fraud offences (or both) and over £41,000 in bitcoin was seized. You can read more here: https://thehackernews.com/2020/12/police-arrest-21-weleakinfo-customers.html

Hackers Steal Mimecast Certificate

Mimecast announced on Tuesday that a digital certificate which allowed customers to connect its products to Microsoft 365 (M365) Exchange had been compromised. The company posted an alert on its website and reached out to the impacted organizations. As a precaution the company asked its customers to delete the existing connection within their M365 and re-establish a new certificate-based connection using the new certificate it has made available. You can read more here: https://thehackernews.com/2021/01/hackers-steal-mimecast-certificate-used.html

WhatsApp -Should I Accept their new Privacy Policy

As promised last week I have been following closely the WhatsApp privacy "ultimatum" story. What is clear is that many are deleting the WhatsApp App without looking at the whole picture. We live in a world where our every move from our internet browsing, shopping habits and even our fitness routines are tracked by technology. Our country may have some of the strictest privacy and data protection laws. But, much of the technologies we choose to use relies on complex "privacy" information and settings which make it difficult for us to actually achieve a "private life".

Privacy researcher Stephanie Hare read the terms and conditions of 13 apps including Teams, Zoom, WhatsApp, TikTok, Facebook, Candy Crush and Twitter (it took her 13 hours in total). She concluded "Consent implies choice, but choice is not what's on offer". Going on to say that the only alternative was to not use the app at all. The article is: https://www.bbc.co.uk/news/technology-55573149

In Early December my blog included "Facebook Accused Of Abusing Its Power To Neutralize Competitors". This highlighted a lawsuit in the US where the government is looking for Facebook to be broken up. The lawsuit aims to set aside the acquisitions of Instagram and WhatsApp and turn them back into independent companies. This is still ongoing.

Since users were delivered the "sign up to our privacy notice or delete the app" message a number of people have rushed to uninstall WhatsApp and migrated to one of the other platforms (Signal or Telegram are often cited as examples). Yet, if they still use Facebook, Google, Facebook Messenger, Amazon, credit cards, reward cards etc. one has to ask why is this new WhatsApp Policy a problem. The content of the message is still encrypted and if the problems is that WhatsApp (and therefore Facebook) will know who you are talking to and how often you do it then surely so does your service provider when you send a text or call via their system. WhatsApp have said the changes do "not change WhatsApp's data sharing practices with Facebook and does not impact how people communicate privately with friends or family wherever they are in the world".

Many haven't even bothered to read the Privacy notice in question before acting so, if you want to read it, here is a link https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies. Ultimately what it says that, as part of the Facebook Group, WhatsApp can receive information from, and share information with other Facebook Companies. They do this in order to help operate, provide, improve, understand, customize, support, and market their Services and offerings, including:

- to improve infrastructure and delivery systems;
- to understand how the Service is;
- to promote safety, security and integrity across the Facebook Company Products;
- to improve their services and your experiences using them (making suggestions for you, personalizing features and content, helping you complete purchases and transactions, and showing relevant offers and ads across the Facebook Company Products);
- providing integrations which enable you to connect your WhatsApp experiences with other Facebook Company Products (For example to connect your Facebook Pay account to WhatsApp or to connect Portal to your WhatsApp account).

What is clear is that for some people (probably those who don't use Facebook, Google or Amazon) will see this as a step too far.

But others will see it as a "necessary evil" so that they can still keep in touch with the colleagues, friends, family and loved ones who use the platform. These people will continue believe that the benefits of WhatsApp (which is after all a free tool) outweigh the potential downsides.

Blogs of the Week

HR Dept - How Employers Can Help Working Parents Through School Closures

This blog discusses ways businesses can help working parents manage the pressures of home schooling. While some businesses are doing everything possible (setting up support clubs for parents and drawing on in-house expertise to help children learn) others are more reticent about granting furlough because of financial pressures, operational impact, or other matters. You can read the full blog here: https://www.hrdept.co.uk/trafford-and-warrington/blog/how-employers-can-help-working-parents-through-school-closures

Altrincham HQ - How To Limit Your Sales & Marketing Distractions In The New Year

Alex starts the blog with "Imagine for a second a distraction free world". Because it's easy in a New Year to chase goals and not really move forward Alex puts forward some things to sense check things. So my top 3 hints are to stop "Chasing The Shiny New Thing", "Choose 2 Marketing Channels That Really Work" and "Audit Your Networking Groups". You can read his full list here: https://altrinchamhq.co.uk/how-to-limit-your-sales-marketing-distractions-in-the-new-year/