

# THURSDAY THOUGHTS

This week Cookies are in the news again, not least because I visited a website for a company who is a “household name” this week and was faced with pre-checked consent boxes, when I raised this with their DPO I was told they were exempt ... they (and you) are not! So “cookie banners”, “cookie walls” and “no to all” cookie consents as well as what you do and do not need consent for are in this week’s Thursday thoughts.

I have also taken some time to review the ICO audit report on the Department for Education (which only came out on the 7<sup>th</sup>). I have some suggestions including what we can all learn from the DfE’s failings and how you can do your own audit and what you may learn.

It is the second week of European Cybersecurity Month so I’ve included pieces on reporting ransomware and why Graham Norton is number one in the “top 10 most dangerous celebrities” according to McAfee. For the golfers amongst you a piece on the new world Golf World Handicap System. Finally, of course, there are the usual updates on tech matters Microsoft 365, the use of Apps that play Netflix in your car via the entertainment system, Facebook and Apple News.

## My “Blog of the Week”

Alex McCann - Imposter Syndrome, Authenticity and Dealing With Social Media

## Cookies

### Cookies and Consent - Websites, Apps and Internet Enabled Devices

I find when I am talking to businesses about consent that there is still a lot of confusion over what you need “Cookie Consent” for and what you don’t. Here is my simple guide to where you need consent and when you do not:

| Consent Required  | Consent Not Required  |
|---|---|
| Cookies that are “not strictly necessary” <ul style="list-style-type: none"> <li>• Advertising Cookies</li> <li>• Analytics Cookies</li> <li>• Personalisation Cookies</li> </ul> | Cookies that are “strictly necessary” <ul style="list-style-type: none"> <li>• Security Cookies</li> <li>• Cookies that make the website work</li> <li>• Fraud Detection Cookies</li> </ul> |

This applies wherever you put something on someone’s device and includes on websites, Apps and Internet Enabled devices. Consent is required BEFORE any cookies that are not “strictly necessary” are placed.

### Cookie Banners

Many organisations are still not using cookie banners correctly. According to some experts up to 90% of websites drop cookies as soon as you arrive on the page. In a lot of cases this is simply because the business hasn’t configured google tag manager to work with their consent banner. So if you are one of the few who clearly gives users the option to decline or accept to cookies - WELL DONE. If you are not then please check if cookies are being dropped prior to consent being given and ensure your google tag manager is set up correctly. This video from Fieldfisher explains all about using cookies: [https://www.youtube.com/watch?v=Nf2vLCcU\\_oA&feature=youtu.be](https://www.youtube.com/watch?v=Nf2vLCcU_oA&feature=youtu.be)



## French Data Protection Authority Amends 'Cookie' Guidelines

The French equivalent of the ICO has published revised guidelines on cookies and other tracking mechanisms with the aim of giving users more control. This ruling reverses a previous ban on using “cookie walls” but it is very clear that the act of refusing cookies must be as easy as accepting them. CNIL recommends that a “refuse all” -button should be offered if an “accept all” -button is used. Why am I telling you this? Because what happens in other countries affects us if we are trading in their country. Moreover, you never know if the ICO will look at the ruling, agree and adopt it in the UK. You can read more here: <https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation>

## How to “Do a GDPR Audit”

I find that GDPR Audits are an incredibly useful way to highlight where the true data protection issues are in an organisation. Often we start with an idea that staff aren't doing things properly and they need remedial training. When you dig deeper you find however that the real reason is that the policies and procedures (especially around data retention and storage) or processes to deal with data breaches/subject access are just not in place. It is therefore very hard for staff to understand what they should do. If you want advice and guidance on conducting an audit yourself I have a number of off the shelf packages you can purchase. Alternatively I am taking bookings for November Audits now. You can direct message me and I will be happy to help.

## ICO - DfE Audit Report

The ICO published quite a damning report on the DfE this week and no it wasn't the exams results fiasco although I am sure we will see that soon. This was the ICO audit report covering a formal Audit of the DfE that took place in February/March 2020. The report highlights a number of areas that we can all learn from:

- It is incredibly important that you have oversight, appropriate documentation and governance systems in place. If you don't have them it is impossible to demonstrate your compliance with GDPR and therefore you will “fail” the accountability principle.
- Information governance works across the whole business and involves all departments, all specialisations and all staff. Often actions in one area directly affect others in the business.
- Make sure you remember to cover both privacy and security by design/by default at the design stage.
- Be aware that there may be internal cultural barriers and attitudes which prevent you from implementing an effective system. You often need to break down internal barriers to implement solutions.
- If you need a DPO, get one. Even if you think it “may be helpful”, get one. But make sure they are suitably qualified and resourced. Dual hatting someone inside the business can result in a conflict of interests. Having someone who isn't trained properly or doesn't have the ear of senior management results in nothing more than a superficial title with no real business benefit. There are many cost-effective alternatives to employing your own DPO including using a consultant or engaging a “DPO As-a-Service”.
- Make sure you have a policy framework and document control system in place.
- Above everything else UNDERSTAND WHAT DATA YOU PROCESS and prioritise the creation of a Record of Processing Activity (ROPA). That way you won't breach Article 30 of GDPR.



- Give your data subjects privacy information at the time of data collection
- Make sure you understand if you are a controller, joint controller or processor.
- Train your staff (about information governance, data protection, records management, risk management, data sharing, information security and individual rights).

## Ransomware Attacks Not Being Reported

Europol has published an assessment that indicates that ransomware attacks are not being reported to the police. They suggest that this is because businesses want to stay out of the public eye as the risk to their reputation is too great. This means that cyber criminals are not being prosecuted as they should be. The UK NCSC Incident Management Team have produced guidance on how to effectively detect, respond to and resolve cyber incidents and have specific guidance on how to prevent ransomware attacks. They urge businesses who have been the victim of fraud or a cybercrime to report it to Action Fraud as soon as possible.

## The Top Ten Most Dangerous Celebrities

Did you know that McAfee produces an annual Most Dangerous Celebrities 2020 study? Nor did I. McAfee research famous individuals every year to reveal which celebrities generate the most “dangerous” results. What they are looking for are search results that bring potentially malicious content which will expose fans’ personal information. This year Graham Norton is at the top of the list which includes (in order) Ricky Gervais, Tom Hardy, Ruth Jones, Mick Jagger, Margot Robbie, Idris Elba, Kate Moss, Bella Hadid and Mary Berry.

What does this mean for you? If you are searching the internet for free content using these names there is a greater chance that you will find malicious content, be led to malicious websites or tricked into downloading a malicious link. So make sure you only click on links to reliable sources.

<https://www.mcafee.com/blogs/consumer/check-out-the-mcafee-most-dangerous-celebrity-2020/>

## Golf World Handicap System

England Golf are planning to implement a “World Handicap System” on 2<sup>nd</sup> November 2020 and have requested affiliated clubs supply an email address and a date of birth for all members so that they can allocate them a “Handicap Index”. As this system includes some automated profiling it is possible that this request could breach Data Protection regulations so many clubs are asking for express consent from members to share this information. I expect to see more in the news about this over the coming weeks: <https://www.englandgolf.org/world-handicap-system-data-faqs/>

## Microsoft 365 Can't be Used in a Privacy Compliant Way

Germany has a “Conference of Independent Federal and State Data Protection Supervisory Authorities” instead of a single data protection authority. This month the conference came to the conclusion that it is not possible to use Microsoft Office 365 in a way that protects users’ privacy. They also think that there is “considerable potential for improvement” in Microsoft Office 365, as a result of “Schrems II”. As with the French ruling on Cookies this will affect businesses working in Germany but has the potential to affect other nations if their authorities agree. You can read the ruling here: <https://www.datenschutz.saarland.de/ueber->



[uns/oeffentlichkeitsarbeit/detail/pressemitteilung-vom-02102020-stuttgart-muenchen-ansbach-wiesbaden-saarbruecken](https://www.bbc.com/news/health-54336423)

## **Apps In Cars – A Good or Bad Thing**

Apps in cars are not new. But the jury is out on whether being able to access things like Netflix in your car via the entertainment system is a good or a bad thing. With many thinking that this is a potential privacy nightmare; the opportunities for hacking is immense. For example in a Tesla Model 3 you can play music straight from your Spotify account, watch Netflix and YouTube on the main screen and play games on the screen when the car is parked or charging. While they cannot at the moment be used while the car is moving who knows what will happen in the future. You can read more here: <https://www.bbc.co.uk/news/business-54336423>

## **Microsoft Faces a Class Action**

In a class action lawsuit against Microsoft it has been alleged that they have been sharing the “content of business customers’ emails, documents, contacts, calendars, and other data with unauthorized third parties for unauthorized purposes” Using this data (which includes location, audio and video files) to develop new products and services.

## **Facebook News**

### **Facebook - Not happy with “The Social Dilemma” documentary**

Facebook is very critical of the Netflix documentary “The Social Dilemma”. Which shows how social media companies manipulate our behaviour for profit and pose an existential threat to democracy. Facebook published a document in response called “What ‘The Social Dilemma’ Gets Wrong”

### **Facebook takes legal action against companies scraping their data**

Facebook has filed a lawsuit against two companies (BrandTotal Ltd and Unimania Inc) for scraping data from Facebook and other platforms so that they could sell “marketing intelligence”.

## **Apple Sues Recycling Firm for Not Recycling Products**

Apple is suing a recycling partner for reselling more than 100,000 iPhones, iPads, and Watches. The company (GEEP Canada, now a part of Quantum Lifecycle Partners) was hired to disassemble at least 11,766 pounds of Apple devices between January 2015 and December 2017. Apple discovered in an audit that 18% of the devices were still accessing the internet.

## **Blog of The Week**

### **Alex McCann - Imposter Syndrome, Authenticity and Dealing With Social Media**

This week David Belling of Subs Altrincham interviewed Alex ahead of World Mental Health Day about Imposter Syndrome, Authenticity and Dealing With Social Media. It’s OK not to be OK. At the moment when we are interacting on line it is it’s easy to turn up and pretend everything is OK and business is going great, whilst in reality everything is an absolute mess. Alex’s blog post is an honest look at the stress of keeping up appearances on social media and how to cope with the difficult days and weeks without completely distancing ourselves from social media. You can read the blog here:

<https://altrinchamhq.co.uk/im-not-ok-imposter-syndrome-authenticity-and-dealing-with-social-media/>

