Thursday Thoughts – 28 January 2021

Today is Data Privacy Day/Data Protection Day. As this last year has been one where the focus has been on online learning, working from home and remote teaching I suggest, instead of the usual doom laden "watch out" messages, we celebrate everything that has gone well over the last year. Whether this is the superhero back office tech staff who have worked tirelessly to keep everyone on line or the millions of individuals who have adapted to new ways of working that no one could have imagined a year ago.

An increasing number of websites seem to be springing up with their Legitimate Interest Cookie permissions automatically turned on. There is no alternative to consent for non-essential cookies and so using the excuse "everyone else is doing it" is no defence. The massive fine for Grindr for doing just that and a forthcoming multi million euro fine for WhatsApp for privacy consent violations should concentrate minds. I predict in 2021 the management of consent and preferences as well as encryption and how society views and treats data protection are going to be key themes. In my quest to find engaging content this week I discovered @RachelTobac and her "Infosec sea shanties".

Blogs of the Week
Lucie Mussett - Introducing our new (NHS) system for patient safety learning
Karen Watson - Welcome To Data Protection Day 2021

Data Privacy/Data Protection Day

This year with the focus on online learning, working from home and remote learning we have seen Data Protection/Privacy become more important in all our lives. Today I'd like to take time to celebrate everything that has gone well over the last year. Congratulating staff for the flexibility with which they have adopted new working processes. Highlighting training, projects and success stories as well as recognising and rewarding particular individuals for effort and expertise, especially those who have gone above and beyond to support everyone else. It shouldn't matter if you have had a disaster (downtime, data breach etc.). Take this opportunity to highlight how your organisation has adapted, changed and dealt with problems. It's certainly a much more positive message than the doom laden "watch out for this latest scam or attack" message which is so often seen.

Cookies and Legitimate Interests

There seems to be a proliferation of websites (especially news media ones) where Cookie permissions have the legitimate interest buttons automatically turned on. As legitimate interests does not exist under ePrivacy law, which is the law that governs cookie/tracker consent, it follows that it is not a valid basis on which to set non-essential cookies. Any personal data acquired or generated by this cannot be lawfully processed. So I recommend you avoid any consent management platform that has a default "ON" position for gathering cookies for legitimate interests. There is no alternative to consent for non-essential cookies.

Consent and Preference Management Platforms

As Privacy becomes more important to businesses the management of consent and preferences is likely to become a core component of marketing platforms. The information gathered is complex and businesses will need to look carefully at the options to ensure that the solutions they select also support the business' privacy strategy. Initiatives such as Google's plan to "kill off" third-party cookies in Chrome in 2022 will no doubt be concentrating minds in boards across the globe. Solutions will need businesses to consider privacy as a continuous engagement piece and build in subject access request and the ability to adjust data sharing preferences into their solutions.

Fines

Grindr fined One Hundred Million Norwegian Krone

A cautionary tale for businesses on the perils of dismissing expert advice in favour of industry-friendly guidance. Just because 'everyone else is doing it' does not make it right. The latest company to fall foul of the GDPR Consent rules is Grindr – in this case for "poor management" of their consent mechanism. Something that should have been clear to them. By making it impossible for users to continue past the privacy settings without accepting behavioural advertising, Grindr left themselves open to a huge fine (approx. £8.5M) from the Norwegian Data Protection Authority.

Authorities in Ireland considering How Much to Fine WhatsApp

Ireland's Data Protection Commissioner has shared with other EU agencies details of their proposed fine for WhatsApp for "failure to live up to the transparency requirements of GDPR". It is estimated that the fine may be between €30 million and €50 million and WhatsApp could also be required to change how it handles its users' data. The main issue is the failure of WhatsApp to properly inform its EU users about how it planned to share their data with Facebook.

News

Encryption and Data Ethics

Service providers need to start to think about data ethics as well as data privacy. Encryption, once the domain of the military and governments, has started to enter the "mainstream" consciousness. Businesses and individuals now pay more attention to things that impact their privacy. As ever there is a fine balancing act between individuals who want more privacy and the governments/law enforcement agencies who are more focussed on content moderation and developing laws to prevent criminality on "encrypted platforms". This potentially could weaken encryption for everyone so it falls to the "experts" to explain what impact there would be on society as a result.

Facebook Cambridge Analytica and the App Audit

The UK Information Commissioner has admitted, to an online harms and disinformation parliamentary subcommittee, that she is unable to answer in public whether Facebook have actually conducted an audit into the activities of Cambridge Analytica as they promised because of an "agreement between the ICO and Facebook". This agreement relates to the ICO litigation against Facebook over the Cambridge Analytica breach (settled in 2019 with payment of £500,000).

The Dangers of Sharing Medical Information

A private COVID-testing facility in the Netherlands considered it was OK to share medical info, national identification numbers and copies of passports with staff via WhatsApp as part of a WhatsApp group. The fact that this information could be forwarded to any contact the employee has on their phone seems to have escaped the company concerned. Unless they have a detailed data protection process in place I cannot see anything other than a fine coming their way. An inadequate cookie banner on their website, no mention of a DPO in their privacy statement and a retention policy that hasn't kept up with changes in the law do not fill me with any confidence.

Privacy Research Project

PrivSec Report is conducting a research project to track privacy employee culture, attitudes and behaviour. The "Global Privacy Culture Survey" will explore accountability, document retention, security, data transfers and breach management and features questions that relate to GDPR as well as other privacy standards and laws from around the world.

Scottish Environmental Protection Agency Ransomware Attack

The Scottish Environmental Protection Agency suffered a Ransomware attack at Christmas - they followed advice and refused to pay. The stolen data (including contracts, strategy documents and databases) has been found on the dark web although it is only accessible with specialised software. The agency made it clear they wouldn't use public finance to pay criminals. They have been quick to recover and analyse data and contact and support affected organisations and individuals.

Rachel Tobac – Infosec Sea Shanties

In my quest to find engaging content this week I discovered @RachelTobac. Who in order to "reach the youth" has decided to make InfoSec sea shanties. The song is a warning to those who reuse their passwords that they may end up pwn'd. Someone else encouraging use of unique passwords, password managers and MFA. Enjoy!: https://twitter.com/i/status/1352409636792492035

Blogs of the Week

Lucie Mussett - Introducing our new (NHS) system for patient safety learning

The new NHS National Patient Safety Management and Learning platform has entered its "beta stage". Described as a "strategic, complex and highly secure service" it has been designed and delivered under exceedingly "challenging" operational conditions. The system aims is to maximise the NHS's ability to learn from when things go wrong. Recording safety events, whether they result in harm or not. This blog is an introduction to PSIMS and an explanation of some of the key features it has. https://www.england.nhs.uk/blog/introducing-our-new-system-for-patient-safety-learning/

Karen Watson - Welcome To Data Protection Day 2021

Karen Watson in this blog discusses the rise of Privacy Tech over the last few years and what she thinks is going to make the difference in 2021. How society views and treats data protection, technology and regulation are key. But will we also see more willingness from the regulators to act and from activists on all sides building awareness and ensuring laws change to meet the needs of the people they protect. You can read the post here: https://mylifedigital.co.uk/welcome-to-data-protection-day-2021/