Data Privacy Detective Podcast – Episode 99: National Cybersecurity Awareness Month

Oct 06, 2022

Categories:

Blogs
Podcast
Technology Blog

October is Cybersecurity Awareness Month

Cybersecurity Awareness Month is co-led by the National Cybersecurity Alliance and the Cybersecurity and Infrastructure Agency (CISA). For more information about ways to keep you and your family safe online visit https://staysafeonline.org/cybersecurity-awareness-month and https://www.cisa.gov/cybersecurity-awareness-month. In this podcast episode, we will cover:

- Instagram fined 405M Euros for GDPR violations – published minors' names and addresses – Meta said it fixed this a year earlier – Anyone under 18 automatically has their account set to private when they join Instagram, so only people they know can see what they post, and adults can't message teens who don't follow them. Meta reviewing the decision.
- Google and Meta were fined a total of $72 million by South Korea's Privacy and Protection Commission for tracking behavior on other sites without consumer approval, then using that data for advertising. Both companies voiced disagreement with the commission's findings and may appeal these largest-ever fines levied by South Korea for privacy law violations.
- The Internal Revenue Service acknowledged Friday that it had inadvertently exposed a batch of taxpayer information linked to some non-profits and other tax-exempt organizations, following a Wall Street Journal report that said as many as 120,000 individuals may have been affected by the error. The accidentally leaked data did not include any Social Security numbers, "detailed account-holder information" or personal income tax returns, the IRS said in a statement, but it included information from Form 990-T, which is used by tax-exempt

entities to report unrelated business income. Only 501(c)(3) organizations are required to make their Form 990-T available for public inspection. An error mistakenly resulted in data from some non-501(c)(3)s also being made available for bulk download through the IRS' search portal for tax-exempt entities, the agency said.

- While its contents might seem unremarkable for China, where facial recognition is routine and state surveillance is ubiquitous, the sheer size of the exposed database is staggering. At its peak the database held over 800 million records, representing one of the biggest known data security lapses of the year by scale, second to a massive data leak of 1 billion records from a Shanghai police database in June. In both cases, the data was likely exposed inadvertently and as a result of human error. The exposed data belongs to a tech company called Xinai Electronics based in Hangzhou on China's east coast.
- China hopes to tighten its cybersecurity laws with higher fines for some violations. If the amendments are approved, fines for critical information infrastructure operators who use products or services that have not undergone security reviews could be 5% of revenue or 10 times their cost. The Cyberspace Administration of China (CAC) said, for example, that it wanted to introduce a penalty that would see operators of critical information infrastructure which used products or services that had not undergone security reviews be fined up to an equivalent of 5% of their previous year's revenue, or 10 times the amount they paid for the product.
- According to Acronis, ransomware losses worldwide are expected to surpass $30 billion by the end of 2023. In the first half of 2022, a majority of incidents involved compromised credentials, though cloud software exploitation and the use of nontraditional entry vectors are also on the rise.
- Lloyd's of London Ltd. has told insurers that nation-state attacks and related losses will be excluded from insurance coverage after 1Q2023. A 2022 court ruling dashed insurers'

hopes that “cyber war” exclusions would let them avoid payment for such losses. There were several reports in Sept of Iranian cyberattacks – Albania is one of the countries complaining.

- Québec’s personal information privacy act takes effect September 22, a provincial statute that supplements Canada’s federal legislation, including the term “confidentiality incidents” and addressing biometric information. Québec privacy law: Certain provisions of the Act to modernize legislative provisions as regards the protection of personal information take effect September 22, 2022.
- Euractiv reports that the EC will introduce its proposal for a Cyber Resilience Act this week. The Act will address cybersecurity issues with consumer connected devices. It will cover “products with digital elements” defined as “any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately”. Products covered by sector-specific rules including medical devices are outside the scope of the legislation. Manufacturers of IoT products will need to comply with security requirements and ensure the confidentiality of data. They will be required to carry out regular stress testing and report issues to a nominated body. Critical products which represent greater risk will have additional obligations and are divided into two classes. Class I includes identity management systems, browsers, password managers, antiviruses and firewalls, VPNs, network management systems, physical network interfaces, routers, and chips used for essential entities as defined in NIS2. Class II, considered as higher risk, includes desktop and mobile devices, virtual operating systems, digital certificate issuers, general purpose microprocessors, card readers, robotic sensors, smart meters, all IoT, routers, and firewalls for industrial use in a sensitive environment. Obligations will extend down the supply chain with penalties for non-compliance of up to €15m or 2.5% of annual turnover, whichever is higher.

- UK – The Telecommunications (Security) Act 2021 (Commencement) Regulations 2022 have been made. They bring the Telecommunications Security Act 2021 (TSA) into force from 1 October 2022. The Electronic Communications (Security Measures) Regulations 2022 under the TSA will come into force on the same date. The TSA strengthens the security framework for 5G technology and full-fiber networks. The Regulations set out specific security requirements for providers. A code of practice provides further technical detail.
- After TikTok allegedly violated U.K. privacy regulations, the Information Commissioner's Office sent a notice of intent including a possible fine of £27 million. The entertainment platform has 30 days to respond to the accusation it gathered private data from users under the age of 13 without their parents' consent.
- California Governor Gavin Newsom has signed The California Age-Appropriate Design Code Act into law. The new legislation, signed by Newsom on September 15, 2022, and passed by the state congress in late August, will implement some of the strictest privacy requirements for children in the US, especially in relation to social media. The law restricts apps' ability to collect data on anyone 18 or younger and requires them to implement their "highest privacy standards" for children and teenagers. Additionally, the law will also require technology-focused companies to incorporate technology to verify a user's age before allowing access to their platforms. "We're taking aggressive action in California to protect the health and wellbeing of our kids," Newsom said in a press release. The move was not well-received by some tech firms, however, who openly criticized it for limiting democratic freedoms. "Although [the legislation]'s motive is well-meaning, many of its chosen means are unconstitutional and risk unintended consequences," commented Chris Marchese, Counsel for NetChoice, a trade association of technology and internet-based businesses. In fact, according to Marchese, the law violates the First Amendment by limiting constitutionally protected speech and infringing on the

editorial rights of websites, platforms, and apps.

- U-Haul International disclosed that it has experienced a data breach of names, drivers' licenses/state IDs but indicated no credit card or financial information was compromised. Rental contracts between November 5, 2021, and April 5, 2022, were accessed, and U-Haul is giving affected customers a year of free identity protection services.
- A teenage cyberattacker gained full access to Uber's systems after impersonating an IT professional from the popular rideshare company to gain VPN access. Though the hack did not expose confidential passenger data, it revealed internal company information, stored administrative account credentials in the clear, and other loopholes in its cybersecurity practices.
- Congress is investigating Meta after The Markup discovered the tech giant's Pixel tool gathered information on users' private health records. According to Georgia Senator Jon Ossoff, the government aims to understand whether Facebook's parent company is collecting or storing patients' personal data accessed through hospital websites. Striking to me – zero about how privacy is invaded by the onslaught of targeted ads as well as phishing, phone calls, etc. – not wanted and caused by sharing of PI to which most people did not knowingly consent – and not to have their personal information shared and sold without express permission. Listen to Episode 98 – Do Not Sell My Personal Information.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

Privacy & Data Security Weekly Update

Need more Data Privacy updates?

FBT Gibbons

Three things that happened recently. Three things you want to know. Three things moving forward. Delivered to your inbox weekly.

Newsletter Sign Up

FBT Gibbons