










Slice of Pii

A review of the past month's news stories related to Personally Identifiable Information (Pii) and other Privacy matters.

LEGEND

-  **SSN SOCIAL SECURITY NUMBER**
-  **CONTACT INFORMATION**
(email address, physical address, telephone and mobile numbers)
-  **GOVERNMENT-ISSUED IDENTIFICATION**
(driver's license, passport, birth certificate, library card)
-  **BIRTH DATE, BIRTH PLACE**
-  **ONLINE INFORMATION**
(Facebook, social media, passwords, PINs)
-  **GEOLOCATION**
(smartphone, GPS, camera)
-  **VERIFICATION DATA**
(mother's maiden name, pets' and kids' names, high school, passwords)
-  **MEDICAL RECORDS INFORMATION**
(prescriptions, medical records, exams, images)
-  **ACCOUNT NUMBERS**
(bank, insurance, investments, credit cards)



LinkedIn Hit With \$335M Fine for Data Privacy Violations

The networking company found liable for illegally gathering user data for targeted advertising by the Irish Data Protection Commission.



Dark Reading Staff, Dark Reading
October 25, 2024

1 Min Read



LinkedIn earned itself a **€310 million** (\$335 million) fine by European Union regulators on Oct. 24 for its violations of the General Data Protection Regulation (GDPR) data privacy rules.

Ireland's Data Protection Commission (DPC) cited concerns regarding the lawfulness, fairness, and transparency of personal data processing for the professional networking site's **advertising purposes**.

As LinkedIn's lead privacy regulator ... found that LinkedIn did not have **lawful basis to be compiling data to target its users with ads**, ultimately breaching GDPR. This investigation was launched following a complaint initially made by the French Data Protection Authority.

Tips ▸ Privacy

SHARE:    

You're being tracked secretly by 3 settings on your phone

By [Kim Komando](#)

October 26, 2024

iPhone

1. Ad tracking

You'll need to change your ad tracking on an app-by-app basis, but Apple makes it easy. Head to **Settings > Privacy & Security > Tracking** to block apps and stop them from asking for permissions in the first place.

2. Significant locations

To opt out and delete your existing data, visit **Settings > Privacy & Security > Location Services > System Services > Significant Locations**.

3. Location tracking

These really are the keys to the castle, and you're in control. Head to **Settings > Privacy & Security > Location Services**. From here, you can disable location tracking across your iPhone or give select apps permission to log where you are at specific times.

Tips ▸ Privacy

SHARE:    

You're being tracked secretly by 3 settings on your phone

By [Kim Komando](#)

October 26, 2024

Android

1. Location tracking

Open **Settings** > **Location** to select which apps are allowed to know your current location. Set this permission for specific apps or completely disable location tracking on your phone.

2. The all-seeing Google

On your phone, go to **Settings** > **Security and privacy** > **Privacy controls** > **Activity controls**. Here, you can stop your data from being logged altogether or set it to auto-delete after a certain time. I like the three-month option.

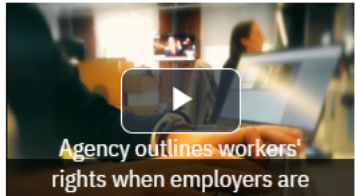
3. App tracking

In the Play Store app, tap your Google profile picture (top right), then choose Personalization in **Play** > **Play personalization** and history to delete your data and stop future tracking.

Employees' right to know: Understanding employers' use of digital surveillance and privacy protections

As more companies adopt invasive employee surveillance tools, workers have a right to know how their personal information is being collected and used.

Posted 3:14 p.m. Oct 25 - Updated 7:02 p.m. Oct 25



By Keely Arthur, WRAL consumer reporter

- **More companies are using digital tools to monitor employees productivity and other activities.** A federal watchdog says that surveillance can not go unchecked.
- **Employee surveillance software can be really invasive.** These programs can record everything from key strokes, to conversations and access your computers camera to take pictures of you.
- The Consumer Financial Protection Bureau [CFPB] announced it is establishing the rights workers have and said employers must follow **Fair Credit Reporting Act** rules. It means employers have to get your consent before getting reports that include personal information collected about you.
- **“Workers shouldn't be subject to unchecked surveillance or have their careers determined by opaque third-party reports without basic protections,”** said CFPB Director Rohit Chopra. “The kind of scoring and profiling we've long seen in credit markets is now creeping into employment and other aspects of our lives.”

UK Introduces New Draft Data Bill

by: Hunton Andrews Kurth's Privacy and Cybersecurity of Hunton Andrews Kurth - *Privacy and Information Security Law Blog-Hunton Andrews Kurth*
© Posted On Friday, October 25, 2024



RELATED PRACTICES & JURISDICTIONS

- Consumer Protection
- Communications Media Internet
- Administrative Regulatory
- Global
- United Kingdom

Print Email Download Info



On October 23, 2024, the UK government introduced the draft **Data (Use and Access) Bill** (the “Bill”) to the House of Lords. The Bill has been introduced by the new UK government, following the lapse of the **Data Protection and Digital Information Bill** introduced by the previous government.

The Bill seeks to **amend several parts of the UK General Data Protection Regulation** and the UK Data Protection Act 2018, including provisions relating to certain **data subject rights (such as the right of access), the principle of purpose limitation in the context of further processing of data, scientific research, international transfers, and automated decision-making.**

It also proposes changes to the structure of the UK data protection authority, the UK Information Commissioner’s Office (the “ICO”). The Bill also introduces significant provisions for digital verification services and digital identities, including requiring that digital providers be certified with the UK government’s “trust framework.”

In a statement published on October 24, 2024, the ICO welcomed the introduction of the Bill and confirmed it will be publishing its response to the Bill in due course.

German company launches 'digital condom'. What is it, how it works

Camdom is straightforward to activate. Before an encounter, users place their smartphones in close proximity and swipe down a virtual button on the app to activate the privacy block. If any attempt to bypass these restrictions is detected, an alarm sounds, notifying both users.

— EDITED BY : SHUBHI MISHRA | OCTOBER 26, 2024 / 12:30 IST



In response to growing concerns about **unauthorised recordings** and the spread of intimate content without consent, German condom company Billy Boy, in collaboration with Innocean Berlin, has launched an app called **Camdom**, a “**digital condom**” that aims to **prevent digital privacy violations during intimate encounters.**

Camdom functions by leveraging Bluetooth technology to block unauthorised camera, video, and microphone access on users’ devices. Felipe Almeida, the app’s developer, explained the purpose of Camdom in a recent statement, saying, “Smartphones have become an extension of our body and we store a lot of sensitive data on them. In order to protect you from the recording of non-consensual content, we’ve created the first app that can block your camera and mic simply through the use of Bluetooth.”

Camdom is straightforward to activate. Before an encounter, users place their smartphones in close proximity and swipe down a virtual button on the app to activate the privacy block. If any attempt to bypass these restrictions is detected, an alarm sounds, notifying both users. The app can also block multiple devices simultaneously, making it adaptable for different settings. **The digital condom aims to tackle the modern issue of revenge porn**

November
2024

Slice of Pii

PSNI disciplines 74 officers who viewed bodycam footage 'for entertainment'

Drugs arrest captured on camera widely shared and watched 248 times 'with little regard for privacy'



More than 70 police officers in Northern Ireland have been disciplined after they accessed **bodycam footage of a drugs arrest** for “**entertainment and amusement**”. During the incident an officer made an error administering a criminal caution, “causing a colleague to laugh out loud”.

The arrest, captured on the body-mounted camera, then appears to have been widely accessed among PSNI officers. The police ombudsman’s office said the PSNI had taken “management action” against 74 officers. Its investigators found that between December 2019 and November 2022 the footage had been watched 248 times by 82 officers and one civilian staffer at 20 different police stations across Northern Ireland.

Most had watched it once or twice, but one officer had watched it 21 times. They also found that only five officers and one civilian staff member had a legitimate reason to access the footage.

Hugh Hume, the chief executive of the police ombudsman’s office, said: “The video may have been viewed for entertainment and amusement, but the officers who did so showed little regard for the privacy of the man being arrested, nor for the emotional wellbeing of their colleague featured in the video.”



A consumer rights group has warned UK shoppers to research their next electronics purchases carefully, after finding evidence of “**excessive smart device surveillance**” from Chinese air fryers and other products.

Which? claimed that smart air fryers from Xiaomi, Cosori and Aigostar all wanted to know customers’ **precise locations**, as well as permission to record audio on the user’s phone.

The Xiaomi app linked to the smart device also connected to ad trackers from Facebook, TikTok’s Pangle ad network and Tencent, depending on the location of said user, the report claimed.

It also said that Aigostar wanted to know the **gender** and **date of birth** of the owner when **setting up an owner account**, and that both it and Xiaomi sent personal user data back to servers in China.

Chauffeur Fined \$10,000 for Sending Obscene Image to Teen via WhatsApp

NOVEMBER 5, 2024 – UPDATED: NOVEMBER 5, 2024 NO COMMENTS 1 MIN READ



A 48-year-old chauffeur has been fined \$10,000 ECC after pleading guilty to sending an obscene image to an 18-year-old female via WhatsApp.

Hudson Prescod, of Vermont/New Montrose, appeared before the Kingstown Magistrates Court on November 5, 2024, where he admitted to misusing a computer system by sending a **menacing image of his genitalia** to the young woman, causing her to feel harassed.

The offence took place on October 28, 2024. Prescod has until October 31, 2025, to pay the fine; failure to do so will result in a one-year prison sentence at His Majesty's Prison.

The End