

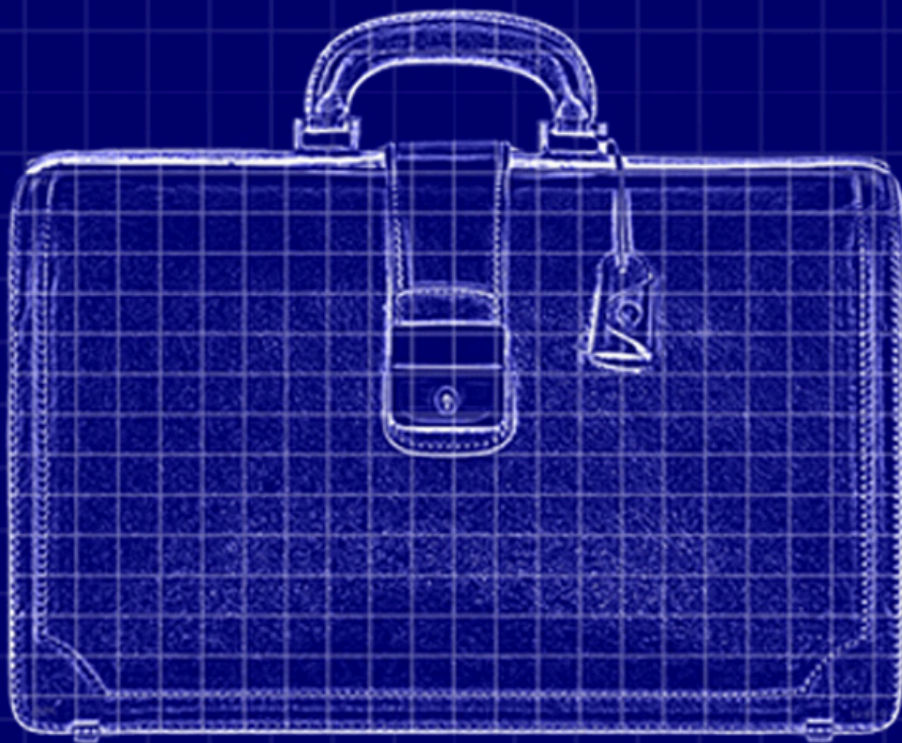
Vol. 1

2025

The Blueprint

PESTLE PROJECT

DECEMBER 2024 - JULY 2025



In this issue:

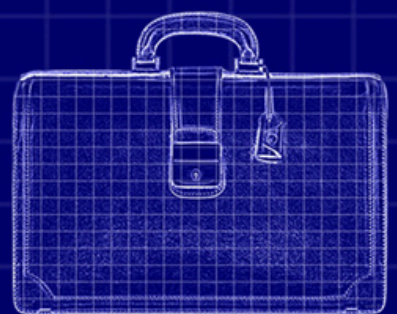
- Femtech apps exploiting your data
- The Getty Images lawsuit
- Governments releasing encrypted data
- Cyberattacks and UK business

FOLLOW US



The Blueprint

TECHNOLOGICAL





The Privacy Fallout of Femtech: How Menstrual Apps Are Exploiting User Data

Rochelle Inbakumar

Introduction


What started as a quiet revolution in reproductive self-care (the rise of menstrual-tracking apps) is now at the centre of a digital privacy storm.

Millions of people in the United Kingdom have downloaded apps like Flo and Clue to track their fertility cycles, manage symptoms, and monitor their overall health. These apps provide valuable insights into one's body, offering control, empowerment, and convenience. Nevertheless, an increasing amount of evidence indicates that beneath their friendly interfaces exists a concerning truth: the information gathered by these applications is being discreetly collected and sold to external parties without user consent.

Summary of Key Developments

A study published by researchers at the University of Cambridge shed light on the hidden world of femtech surveillance. The researchers analysed the data flows and privacy policies of 30 of the most popular menstrual apps in the UK app marketplace. According to the report, many apps collect and transmit sensitive health data to advertisers, analytics firms, and other opaque data brokers. Privacy policies were described as excessively long, jargon-laden, and deliberately confusing. One app's privacy document reads over 14,000 words and requires a postgraduate reading level.

The findings have prompted privacy watchdogs, legal experts, and women's rights groups. The UK's Information Commissioner's Office (ICO) has stated that it is reviewing the Cambridge findings and has reminded app developers of their obligations under the UK General Data Protection Regulation (UK GDPR).



When data from menstrual-tracking apps is leaked, it can reveal highly personal information, such as sexual activity, pregnancy status, or mood patterns that many users would never knowingly share. This exposure may result in significant repercussions, including workplace discrimination, challenges with insurance providers, and potential legal liabilities in certain regions. Furthermore, it paves the way for targeted advertising, erodes trust, and diminishes individuals' autonomy over their bodies and health data.

Analysis of Key Developments

Geographical Reach

While the UK is the focal point of this crisis, the problems are global in scope. Numerous apps involved in this matter are created in the United States, Israel, or Southeast Asia, frequently beyond the jurisdiction of UK regulatory authorities. Nevertheless, their offerings are readily accessible to users in the UK and frequently depend on British cloud service providers and advertising networks. This international framework complicates the issue of accountability and prompts pressing inquiries regarding cross-border data transfers. Are foreign developers obligated to comply with UK GDPR standards when handling reproductive data? Moreover, if not, who ensures users are protected?

Strengths and Weaknesses

The UK GDPR and the Data Protection Act 2018 provide theoretically robust safeguards, particularly for sensitive data types such as health records. They establish principles of informed consent, data minimisation, and purpose limitation. However, in practice, the enforcement of these protections remains weak. App developers frequently employ "dark patterns" - manipulative design features encouraging users to share their data. One high-profile example involved an app offering cycle insights only after users agreed to full tracking permissions. Another forced users to tap through multiple confusing pop-ups with misleading "Accept All" options. While these strategies may be legally defensible, they erode user trust and distort consent.



Have the Issues Been Remedied?

As of June 2025, no meaningful regulatory sanctions have been imposed. The ICO is conducting an ongoing review, and several developers have taken modest steps, including revising user interface (UI) prompts and shortening privacy policies. However, critics argue that these changes are primarily for show. Without real consequences or rules that require companies to be transparent by design, not much is likely to change across the industry.

At the same time, a growing grassroots movement is starting to push back. Users are beginning to delete popular apps in favour of open-source or feminist-designed alternatives that promise no data collection, encrypted storage, and offline functionality.

Examples of Similar Instances from Other Jurisdictions

The United States offers a stark illustration of what can go wrong. Privacy fears spiked after the Supreme Court overturned *Roe v. Wade* in 2022. Advocacy groups reported cases where data from menstrual apps was used in legal investigations related to abortion. Some developers responded by offering anonymous or encrypted modes, but many moved servers offshore to reduce liability.

In Germany, the Federal Commissioner for Data Protection has issued formal advisories cautioning citizens against using apps hosted outside the European Union. France and Spain followed with consumer warnings. South Korea's Ministry of Science has since launched a femtech certification programme requiring domestic data storage and independent audits.

These examples illustrate how global regulators are grappling with the ethical frontiers of femtech, but few have found a lasting solution.



Legislative Reach

In the UK, the relevant laws, GDPR and the Data Protection Act 2018, explicitly define reproductive and biometric data as requiring heightened protection. However, the absence of enforceable design standards allows loopholes to persist. The Data Protection and Digital Information Bill, presently debated in Parliament, could change the current framework again. Supporters claim it simplifies compliance for new businesses. Conversely, critics warn that it may weaken rights-based protections, prioritising economic growth over individual security.

Retained Law: What Are the Implications?

Since Brexit, the UK has retained much of the EU's data regime but is increasingly under pressure to chart its path. If the UK diverges too far, it risks losing its data adequacy agreement with the European Union, a critical asset for cross-border commerce. People in the UK who use apps developed or hosted in the EU may face legal grey areas, as they are unsure of the privacy protections that apply to them. As the UK looks to reform its data laws, handling sensitive information (such as reproductive health data) could hinge on how closely those reforms align with European standards. If the UK weakens its privacy regulations, it might reduce the ability to enforce protections and attract bad actors looking to exploit looser rules.

Conclusion: Retrospective Summary and What Might Happen in Future

The rise of menstrual-tracking apps highlights both the potential and the challenges of digital health. While these apps provide valuable tools for users to understand their bodies, they also reveal a systemic failure in oversight, transparency, and ethics.

Despite existing legislation, enforcement has not kept up with the rapid growth of femtech. Without adequate regulation, an alternative market is emerging - one focused on ethical design, user ownership, and gender-inclusive technology. Female-led startups are leading the way with privacy-first models, and user interest in these options is rising.



Some experts suggest that this moment calls for a public-sector solution, such as an NHS-supported app that prioritises clinical accuracy and user trust over profit. If the UK aims to be a leader in digital health, it must move beyond mere regulatory measures. Protecting reproductive data is not just a compliance issue; it is a matter of human rights. The path forward will require bold policy actions, industry accountability, and a cultural shift emphasising bodily autonomy in the digital age.



Brand Theft or Innovation? The Case That Could Rewrite AI Law

Gwyn Velasco

Introduction

In early 2023, a legal showdown began between Getty Images, a leading international stock photo agency, and Stability AI, the developer behind the image-generating artificial intelligence tool Stable Diffusion. Filed in the UK High Court, Getty's lawsuit represents one of the first major tests of how existing intellectual property (IP) law applies to generative AI. At the heart of the dispute are two key allegations: that Stability AI unlawfully used Getty's copyrighted images for training its AI model and that its outputs dilute Getty's brand by replicating watermarked content.

As AI-generated media becomes increasingly accessible, the case raises urgent questions around fair use, consent, and what it means to "copy" in the age of machine learning. The English hearing, which is still ongoing as of July 2025, could become a global benchmark for regulating the use of training data and AI outputs.

Summary of Key Developments

In January 2023, Getty Images filed a lawsuit in the High Court of Justice in London accusing Stability AI of: infringement of copyright, by allegedly copying over 12 million Getty photos without consent to train Stable Diffusion and also breach of trademark and passing off due to outputs from Stable Diffusion that mimicked Getty's distinct watermark, potentially misleading the public and damaging brand reputation.

Notably, Getty dropped the copyright infringement claim in the UK case by late 2024, narrowing its focus to trademark issues and "unfair extraction and use of content" that would otherwise require licensing under UK IP law. In a press statement, Getty called the AI firm's behaviour "parasitic", accusing it of dragging its brand "through the gutter" by associating it with low-quality or distorted images bearing counterfeit watermarks.



Meanwhile, Stability AI has argued that training an AI system on publicly available content is lawful, and any replication of watermarks is unintended and sporadic. The company maintains that its training practices are in line with existing copyright exceptions, such as "text and data mining" (TDM) allowances under UK law. This is particularly relevant, given that the UK had previously proposed looser TDM exemptions before reversing course following industry backlash.

Analysis of Key Developments

The case has emerged as a flashpoint in an increasingly heated debate about ownership and originality in AI. While Getty's original US case focused squarely on copyright, its UK strategy underscores a different legal vulnerability: the use of protected trademarks and the implications of AI models generating images that appear to come from a legitimate brand but are unauthorised and distorted.

This is legally significant because UK intellectual property law, unlike the US, lacks a strong "fair use" doctrine. Instead, it relies on narrower exceptions such as "fair dealing," which are less accommodating to the mass use of protected works in AI training. Getty is leveraging this difference by emphasising reputational harm and brand confusion, areas where UK courts have been historically more sympathetic to rights holders.

At the same time, the controversy reflects deeper uncertainty about the transparency and accountability of large AI models. Stability AI, headquartered in London, has acknowledged that it did not obtain permission from Getty or similar rightsholders to include their work in its training data. However, the company insists that its model does not store or reproduce training images directly, making it challenging to draw a clear distinction between influence and infringement.

Further complicating the matter is the AI's ability to replicate Getty-style watermarks, suggesting not just conceptual inspiration but a potential attempt to pass off AI-generated content as licensed Getty material. Getty's legal team argues this erodes consumer trust and creates a "confusing digital marketplace" where fake content appears indistinguishable from the real.



Legal and Industry Implications

This case is unfolding against a shifting regulatory landscape. While the UK government initially signalled support for relaxed rules on text and data mining to support AI development, it reversed course in 2023 under pressure from creative industry groups, including Getty. This reversal now strengthens Getty's position and may open the door to licensing regimes or AI training royalties, similar to those in the music and video streaming industries.

Additionally, the UK IPO (Intellectual Property Office) is currently reviewing public consultation feedback on AI and IP, with a white paper expected by late 2025 that could reshape how data scraping and generative models are treated in law. A ruling in Getty's favour would likely accelerate such reforms, giving rights holders a clearer legal toolkit to challenge AI companies and compelling AI developers to rethink training protocols entirely.

This case also intersects with consumer protection law, with growing attention from regulators such as the Competition and Markets Authority (CMA) on whether AI models distort market integrity by producing deceptive or low-quality imitations.

Conclusion

Getty Images vs. Stability AI could become the UK's most consequential legal case on generative AI to date. It highlights the tension between innovation and accountability, setting the stage for how copyright, trademarks, and consent will be interpreted in a post-AI creative economy. While a final ruling is still pending, the outcome may determine whether generative AI remains a grey zone of "free-for-all" training or whether it is reined in by conventional IP protections. For now, one thing is clear: the legal foundations of AI development are no longer theoretical; they are under cross-examination.



Code of Silence: The UK Government's Digital Backdoor Battle with Big Tech

Rochelle Inbakumar

Introduction

In November 2024, a quiet directive from the UK government triggered a global debate that now sits at the heart of one of the most consequential privacy battles of the decade. Apple, one of the world's most valuable companies, was ordered by British security services to provide a secret backdoor to its encrypted iCloud backups. This could expose the private data of billions of people. Instead of silently complying, Apple took the extraordinary step of suing its regulator. WhatsApp, itself no stranger to encryption wars, has now joined with Apple. Together, the two tech titans have thrown down a marker: some doors should stay locked for good.

Summary of Key Developments

The order arrived in the form of a Technical Capability Notice (TCN), issued under the Investigatory Powers Act - a sweeping surveillance law often described, and not entirely affectionately, as the "Snoopers' Charter". In effect, the Home Office demanded that Apple re-engineer its Advanced Data Protection (ADP) feature so that UK security agencies could peer inside a user's iCloud backup, should a warrant be granted.

Apple's response was remarkable. It quietly deactivated the ADP feature for UK-based iCloud accounts, stating that it would not compromise the security of its global user base by introducing a vulnerability that could be exploited by criminals, rogue insiders, or even foreign states.

In June 2025, WhatsApp applied to intervene in the case, describing the government's demand as an existential threat to end-to-end encryption, a core USP of its entire brand. In a rare twist, the Investigatory Powers Tribunal ruled that certain aspects of the case could be discussed publicly, defying the usual wall of secrecy surrounding surveillance litigation. As the case moves forward, the stakes could not be higher: for tech firms, for civil liberties, and for digital privacy itself.



Analysis of Key Developments

Geographical Reach

This is not just a UK story; the directive's reach is potentially global. Apple's iCloud infrastructure is not neatly divided by borders; a flaw introduced for one jurisdiction can quickly become a vulnerability everywhere. US senators have already voiced concerns that the UK's action would conflict with the CLOUD Act, which regulates foreign governments' access to data stored by US companies. Meanwhile, EU privacy campaigners argue it risks undermining the GDPR's protections, creating a ripple effect that could embolden more governments to demand the same. When it comes to encryption, there is no such thing as a local backdoor.

Strengths and Weaknesses

Apple and WhatsApp weigh technical reality on their side. The argument is simple: once you create a way in, you cannot guarantee who walks through the door. History is littered with cautionary tales. Proponents of backdoors often dismiss such risks as hypothetical, but the track record says otherwise.

The government, on the other hand, argues that complete encryption obstructs justice, particularly when it comes to counterterrorism or child sex abuse investigations. Ministers maintain that TCNs are used rarely and under judicial examination, and that oversight procedures are strong. Nonetheless, many contend that the Investigatory Powers Act is excessively clandestine and expansive. The Tribunal's partial lifting of the veil suggests even the judges see the need for sunlight.

Have the Issues Been Remedied?

No easy fix is on the table. By turning off ADP for UK users, Apple has created an awkward patchwork: a British lawyer or doctor storing sensitive client data in iCloud is now less secure than their peers abroad. WhatsApp (for now) continues to offer end-to-end encryption in the UK, but if the case goes against them, that could change. Both companies are clear: they would rather withdraw services than compromise encryption. In reality, they might face fines or be forced to defy the law, risking a constitutional clash between privacy rights and national security powers.



Examples of Similar Instances from Other Jurisdictions

This standoff is hardly unique to the United Kingdom. In 2016, the FBI's attempt to force Apple to unlock the iPhone of the San Bernardino shooter fizzled out when the agency found another way in, but the legal precedent was left unsettled. In India, the government has proposed similar powers. Brazil has shut down WhatsApp multiple times over encryption disputes. Even the EU has given thought to the idea of "lawful access" proposals, but never fully crossed the line. In Russia and China, by contrast, tech firms have little choice but to comply with state surveillance demands. The question facing Britain is whether it wants to be grouped with liberal democracies that uphold digital privacy, or something else.

Legislative Reach

The Investigatory Powers Act remains one of the most far-reaching surveillance frameworks in the democratic world. Its supporters say it is an essential tool for keeping people safe. Nonetheless, the Tribunal's willingness to allow partial transparency in this case hints at unease with its secrecy provisions. If Apple and WhatsApp succeed, it could force a rethink of how TCNs are issued, or at the very least how they are scrutinised. The UK's departure from the EU sharpens this tension further: the country's divergence from GDPR norms risks eroding trust in how data is handled and secured.

Retained Law: What Are the Implications?

Brexit means the UK is no longer beholden to the EU's evolving digital privacy regime. That freedom cuts both ways. On the one hand, it enables Parliament to legislate boldly in the interest of national security. On the other hand, it risks alienating international partners and businesses that depend on strong privacy assurances.

Law firms, financial services, and healthcare providers (sectors that handle vast amounts of sensitive data) could find themselves at odds with clients who are unwilling to host information on British servers. In an economy built on digital trust, reputational harm can be a slow-rolling disaster.



Conclusion: Retrospective Summary and What Might Happen in Future

This case may prove to be a defining moment in the endless tug-of-war between privacy and security. If the Tribunal sides with Apple and WhatsApp, the judgment will send a message that encryption must remain inviolate, even when uncomfortable for governments. If the Home Office prevails, other countries will surely take note, and the backdoor once opened will never truly close again. For now, billions watch from behind their screens, trusting that the locks they rely on will hold. The question is whether they can still do so.



The Next Big Threat Isn't Physical: The Growing Threat of Cyberattacks on UK Business

Gwyn Velasco

Introduction

In April 2025, Marks & Spencer (M&S) and the Co-operative Group (Co-op) were the subjects of cyberattacks. These incidents disrupted daily operations, raised concerns around data protection and exposed weaknesses in their IT infrastructure.

These attacks reveal critical shortcomings and vulnerabilities within technology infrastructure and data protection law. These events have sparked wider discussions about the current strength of cybersecurity protocols in the retail sector, particularly regarding resilience and regulatory compliance in the face of increasingly complex threats. As a result, both organisations are now working closely with the National Cyber Security Centre (NCSC), the Information Commissioner's Office (ICO), and cyber insurers.

Summary of Key Developments

On 22 April 2025, what initially appeared to be a minor payment issue escalated into a ransomware incident for M&S. Therefore, their online shopping platform was taken down for more than six weeks. Meanwhile, the company confirmed that customer data, including names, email addresses and order histories, had been accessed. Although no payment or password information was compromised, the confidence of customers was severely shaken.

Subsequently, Co-op detected a similar cyber threat and, in response, decided to shut down part of its IT network as a countermeasure. Physical stores remained open, and payment systems were unaffected; however, like M&S, personal data for a substantial number of members, both current and former, was accessed. It was later revealed that the group responsible for the cyberattacks on both UK retailers was Scattered Spider, which had previously targeted companies in the US.



Analysis of Key Developments

Geographical Reach

The cyberattacks had a widespread impact across the UK. Customers across the country were affected by the suspension of M&S's online platform because its delivery operations are nationwide. The Co-op shared a similar concern: operational challenges across its network of over 2,000 stores had harmed both its operations and its national reputation.

It is important to note that the attacks on M&S and the Co-op are far from isolated cases. The Scattered Spider is believed to be responsible for hacking major U.S. companies, including MGM Resorts and Caesars Entertainment. Whilst in the UK, organisations such as WHSmith and Transport for London have also experienced recent cyber incidents. These cases reflect a trend of sophisticated cyber threats targeting high-traffic consumer platforms that harbour valuable personal data for those seeking to exploit it.

The ICO is actively investigating the breaches and has the power to impose substantial penalties under the UK GDPR. The NCSC and the National Crime Agency are also involved in efforts to underscore the serious nature of these attacks and the growing role of public agencies in supporting private sector cybersecurity. In which 4 people have already been arrested in relation to the cyber attacks.

Retained Law

The GDPR remains a law under the Data Protection Act 2018[6] despite the UK's departure from the EU, meaning M&S and the Co-op are still legally required to notify the ICO within 72 hours of discovering a data breach, whilst also maintaining appropriate technical and organisational safeguards to protect personal data. If these companies are found to violate their obligations, they risk facing legal penalties, financial fines, consumer claims and heightened scrutiny from insurers.



Strengths and Weaknesses

When the breaches were discovered, both companies responded. M&S suspended its online platform, and Co-op deactivated a portion of its IT systems to contain damage and demonstrate effective crisis management. M&S restored its online services by 10 June 2025, but only partially. Features such as click-and-collect and delivery to Northern Ireland were not immediately available. Similarly, the Co-op's internal systems were gradually brought back online. However, the full scale of its data breach is still under investigation. These steps have been vital in recovering, yet they can be seen as short-term due to concerns regarding lasting structural improvements to prevent future cyberattacks.

However, it exposed significant cybersecurity vulnerabilities in the UK technology infrastructure. For instance, M&S's dependence on a third-party IT vendor created a weakness that Scattered Spider exploited to gain access to personal data for many individuals. The events that transpired help to highlight a broader challenge within retail cybersecurity: inadequate vetting and oversight of external partners, which can ultimately leave organisations exposed.

Conclusion: Retrospective and Future Outlook

The recent cyberattacks on M&S and the Co-op have demonstrated the vulnerability of even the most established retailers, and the attacks are becoming increasingly sophisticated at an alarming rate. M&S reportedly lost around £300 million during its website's offline period, reflecting the sheer financial cost of such disruptions. It is becoming increasingly clear that cybersecurity is no longer a back-office IT matter, but has become central to legal compliance, reputational management and long-term business viability. There are still significant concerns about due diligence, third-party risk, and data governance.

Looking ahead, stricter regulatory expectations, more thorough vetting of supply chains and an even greater emphasis on board-level accountability are needed. The recent attacks represent a turning point for how the UK retail sector should approach cybersecurity and data protection. Whether genuine reform will take hold or cybersecurity will remain a reactive patchwork remains to be seen.

The Blueprint

END OF GUIDE

