Considus

TECHNICAL WHITE PAPER

Catchlight for iPhone

Protecting your notes without Advanced Data Protection

What the withdrawal of Advanced Data Protection actually cost UK iPhone users, why Notes and Reminders were two of the ten categories affected, and what is still in your hands.

Applies to Catchlight 1.0

Introduction

In February 2025 a feature disappeared from British iPhones and most people who lost it never knew they had it.

Advanced Data Protection was Apple's opt-in setting that put end-to-end encryption across most of iCloud. Turn it on and Apple held no key to your photos, your files, your backups or your notes. The UK Home Office served Apple with a notice under the Investigatory Powers Act requiring access to that data, and Apple's answer was to withdraw the feature here rather than build the access. New UK users could no longer switch it on. Existing ones were told to switch it off themselves.

Apple's own words, still on its support pages, are that it is "deeply disappointed that our customers in the UK will no longer have the option to enable Advanced Data Protection (ADP)". That is not a company being coy about a product decision. That is a company saying it was made to do this.

Eighteen months later the legal question is still open, the feature is still gone, and the practical position for a British iPhone owner has not moved an inch. What has changed is that the case is now being heard in public, so for the first time the facts are checkable rather than briefed.

This paper is about what that actually costs you, and what you can do about it. Not the constitutional argument, which other people own and do better. The narrower question of where your notes are now, who can reach them, and what is still in your hands.

Two of the ten iCloud categories that lost end-to-end encryption in the UK are Notes and Reminders. That is not a side effect of this dispute. For anyone who keeps their thinking on their phone, it is the whole of it.

What this covers, and what it doesn't

This covers the position of a UK iPhone user's notes and reminders after ADP, what Apple's Standard Data Protection does and does not do, what survived the change untouched, and the practical options a person actually has. Section 7 scores Catchlight against the same questions, including where it loses.

Some things are not here. This is not legal advice, and I am not a lawyer. It does not argue whether the Investigatory Powers Act is good law or bad law, which is advocacy rather than product documentation, and the people who do that properly are cited in the references instead. It does not speculate about what the Tribunal will decide.

It also does not tell you what is in the notice. Nobody outside the case knows, the Tribunal is proceeding on assumed facts rather than the classified specifics, and a paper that guessed would be worth less than one that says so.

This document is news-shaped and that is a known hazard. A paper that rots is worse than no paper, because the rot is dated and discoverable. Section 9 carries the revision commitment that answers it, and the version history at the end is where you check whether it has been kept.

1 What actually happened, with dates

The public record is unusually clear for a case largely conducted in secret, because the Tribunal itself ruled that it could not all stay secret.

DATE	WHAT HAPPENED
February 2025	The Washington Post reports that the Home Office has served Apple with a Technical Capability Notice
February 2025	Apple withdraws Advanced Data Protection for new UK users. Existing users are given time to turn it off themselves
April 2025	The Investigatory Powers Tribunal publishes a judgment rejecting the government's argument that the existence of the case should stay secret
July 2025	The Tribunal directs a seven-day hearing, listed for early 2026
October 2025	The UK withdraws the original notice and issues a second one. Apple's challenge to the first is dismissed
February 2026	Privacy International files an amended complaint
August 2026	Apple files a fresh claim against the rewritten notice. A case management hearing is set for September 2026
December 2026	The substantive hearing is currently listed

The claim is IPT/25/83/CH. The claimants are Privacy International, Liberty and two individuals. The respondent is the Home Office, and Apple is a party alongside them.

The instrument is a Technical Capability Notice under section 253 of the Investigatory Powers Act 2016. That section lets the Secretary of State require a telecommunications operator to maintain a technical capability to give effect to a warrant. It does not itself authorise reading anybody's data. It requires that the ability to do so exists and is kept working.

That distinction matters more than it sounds, and section 3 is about why.

2 What you lost, exactly

Apple's own documentation is precise about this, which is worth saying because most reporting was not.

Ten iCloud data categories lost end-to-end encryption for UK users. iCloud Backup, iCloud Drive, Photos, **Notes**, **Reminders**, Safari Bookmarks, Siri Shortcuts, Voice Memos, Wallet Passes and Freeform. These now fall under what Apple calls Standard Data Protection, where the data is encrypted but Apple holds a key.

Fifteen categories were already end-to-end encrypted by default and are untouched. iCloud Keychain and Health are the two Apple names. Your saved passwords did not become readable. Neither did your health data.

iMessage and FaceTime remain end-to-end encrypted globally, including here. Apple says so plainly and it is worth repeating, because a great deal of coverage in February 2025 left people believing their messages had been opened up. They had not.

So the shape of the loss is specific. Not everything, not messages, and not passwords. But your notes, your reminders, your photos and your whole device backup moved from a category Apple cannot read into a category Apple can.

Notes and Reminders are the two that matter for this paper, and it is worth sitting with why. A notes app is where people put the things they have not decided to say yet. Half-formed opinions, medical worries typed at two in the morning, the draft of a difficult message, the list of reasons for leaving. That content is not sensitive because it is scandalous. It is sensitive because it is unfinished.

3 Standard Data Protection is real encryption, and that is not the point

It would be easy, and wrong, to write this as though your notes are now sitting in plain text on a server somewhere.

They are not. Standard Data Protection encrypts your data in transit and at rest. The infrastructure is serious and the people who built it are good at their jobs. If somebody steals a hard drive out of an Apple data centre they get nothing useful.

The difference is who holds a key, and it is the only difference that matters here. Under Advanced Data Protection, the key lived on your devices and Apple had no copy. Under Standard Data Protection, Apple holds a key. That means Apple can be required to use it.

This is the same test the rest of this programme keeps coming back to, and it is the whole of the argument. **An organisation that can hand your data to somebody else will eventually be asked to.** Not necessarily by a government, and not necessarily with bad intent. A court order, a mistaken account flag, a compromised internal tool, a rogue employee. The mechanism differs and the property is constant: a key that exists can be used, and a key that does not exist cannot.

Nothing in that paragraph is a criticism of Apple, whose behaviour throughout this has been about as good as a company's can be. They were asked for a capability, they declined to build it, and they withdrew the feature rather than quietly weaken it. Withdrawing it was the honest move and it cost them.

4 What a Technical Capability Notice is, and what it is not

Some care is needed here, because this is the part most often reported loosely.

A notice under section 253 requires an operator to **maintain a capability**. It is a standing engineering obligation, not a search warrant. Reading a particular person's data still requires the separate authorisation the Act provides for, with its own tests and its own oversight.

So "the government can read your notes" is not an accurate summary. What is accurate is narrower and, I think, more unsettling once you look at it directly. The dispute is about whether a capability must exist at all. Once it does, everything downstream depends on the rules for using it, on the people applying those rules, and on nothing going wrong for as long as the capability exists.

There is a second feature of these notices worth knowing. **They come with a duty of secrecy.** A company served with one is generally not permitted to say so. The reason the public knows about this at all is that it leaked to a newspaper, and the reason the case is being heard in the open is that the Tribunal decided in April 2025 that the government's argument for total secrecy went too far.

That is not a small thing. It means the ordinary answer to "has this company been served with a notice?" is that they cannot tell you, and a company that has not been served often cannot usefully distinguish itself from one that has.

Which leads to the only durable answer available to a person choosing software.

5 The question worth asking is architectural

If a company cannot always tell you what it has been asked to do, and cannot always tell you it has been asked at all, then a promise about future behaviour is not worth much. Not because anyone is lying, but because the promise is not theirs to keep.

What can be assessed is what the software makes possible.

An organisation cannot be compelled to hand over a key it does not have. That is not a policy, a value or a commitment. It is a property of a system, and it holds regardless of who runs the company next year, what jurisdiction it moves to, or what it is served with.

So the question to put to any app holding your private writing is not "would you resist an order?" It is: **could you comply if you wanted to?** For most apps the answer is yes. That does not make them dishonest, or even a bad choice. It makes them a different kind of choice, and one worth making knowingly.

Section 6 is what to do about it. Paper 3 in this series, How to tell whether a notes app is actually private, is seven tests you can run yourself on any app to find out which kind you are holding.

6 What a UK iPhone user can actually do

Five practical options, roughly in order of how much they cost you.

Understand what is still protected, and stop worrying about it. Passwords in Keychain and Health data never lost end-to-end encryption. Neither did iMessage or FaceTime. If your worry was your messages, your worry was misplaced, and there are better things to spend it on.

Move the genuinely private writing off iCloud Notes. This is the direct answer and it is less painful than it sounds, because it does not have to be everything. Most people have a small amount of writing that is properly private and a large amount that is shopping lists. Moving the first is a short afternoon.

Turn off iCloud Backup, or accept what it means. This is the one people miss. A device backup contains a copy of a great deal, and iCloud Backup is on the list of ten. An app can exclude its own data from the device backup, which is what Catchlight does, but that only covers that app.

Use an app that holds no key. Several exist and Catchlight is one of them. Section 7 is honest about where ours is weaker than the alternatives.

Keep a local copy of anything you would grieve. This is not about this dispute at all. It is true every year regardless of the law, and the people who lose writing overwhelmingly lose it to a forgotten password or a dropped phone rather than to a government.

What I would not recommend is a VPN, which does nothing about this whatsoever, or moving to a provider in a jurisdiction you like the sound of, which trades a known legal regime for an unknown one and usually a smaller engineering team.

7 Catchlight against the same questions

I would have no business publishing this without answering it about our own app.

QUESTION	CATCHLIGHT
Does the maker hold a key to your notes?	**No.** There is no account and no server. Your content is encrypted on the device under a key derived from a phrase only you hold
Could the maker comply with a notice for your content?	**No, for the content itself.** There is nothing to hand over. The architecture is in The Catchlight encryption architecture
Is your data in iCloud?	**Possibly, and encrypted before it gets there.** Sync writes to a folder you choose, which can be iCloud Drive. The provider receives ciphertext
Is it in your iCloud Backup?	**No.** The database and its sidecar files are excluded from device backup deliberately
What can the provider still see?	**File count, file sizes and its own timestamps.** Not a word of content, and since the index is encrypted, not how many notes you keep or what you deleted
Has Considus been served with a notice?	**No.** And you are right to notice that a company under one might not be able to say so, which is exactly why the architecture matters more than this row

Where Catchlight is weaker than Apple Notes. It is one app from a small studio, not a platform feature with Apple's engineering behind it. It is iPhone only. Version 1.0 syncs one device. There is no independent security audit, and paper 1 section 11 says so at length rather than burying it. If you lose your devices and your phrase together, the writing is gone, and nobody can get it back for you, including me.

Those are real costs and for some people they will outweigh the benefit. That is a reasonable conclusion to reach and this paper is not written to argue you out of it.

8 What this does not protect you against

Read this section with section 6, because either half alone gives a false picture.

None of this helps with an unlocked phone. Encryption protects data at rest and in transit. It does nothing for a screen somebody is already looking at, and that remains the most likely way anybody reads your notes.

None of this is a defence against a lawful order aimed at you. If you are the subject of an investigation, the route to your writing is your phone and your cooperation, not a cryptographic attack. Paper 2, Who might read your notes, takes that case seriously and says plainly where the architecture stops helping.

Metadata survives everything discussed here. Whoever hosts your files can see how many there are, how big they are and when they last changed, whatever app wrote them.

The legal position may change while you are reading this. A Tribunal ruling, a withdrawn notice, a new one, or a change in the Act could each move it. That is the nature of writing about a live case and it is the reason for the next section.

9 The revision commitment

This document describes a dispute that is still running. Section 3 of the white paper programme is explicit that a paper which rots is a liability rather than an asset, and news-shaped material is the obvious way that happens.

So the commitment is stated here rather than assumed, and it is checkable.

This paper is revised whenever the case materially moves. A hearing that produces a ruling, a notice withdrawn or reissued, or a change to Apple's UK position each trigger a new version. Every revision adds a dated row to the version history below, and a version that is more than three months behind a known development is a defect in this document, not a detail.

If you find that has slipped, the report form at catchlight.app/support reaches me and does not ask who you are.

10 Don't take my word for any of it

Every factual claim above is sourced in the next section, and three of them are worth checking yourself because they are the load-bearing ones.

Apple's own support page lists precisely which ten categories lost end-to-end encryption and which fifteen did not. It is Apple's document, not journalism about it, and it names Notes and Reminders.

The Tribunal's April 2025 judgment is public and is the reason any of this can be discussed. It is the document that decided the case could not be entirely secret.

Privacy International publishes its own case page, as a party to the claim, with the case reference and the procedural history. A party's own account of a live case is not neutral, and it is a great deal closer to the source than a summary of a summary.

References

Primary and party sources

Apple, "Apple can no longer offer Advanced Data Protection in the United Kingdom to new users"

Privacy International, PI Apple TCN Challenge, claim IPT/25/83/CH

Investigatory Powers Act 2016, section 253, Technical capability notices

Investigatory Powers Tribunal

Companion documents

The Catchlight encryption architecture, for how the key hierarchy makes the claims in section 7 structural rather than promised

Who might read your notes, for the adversary-by-adversary version, including the compelled-disclosure case

How to tell whether a notes app is actually private, for the seven tests that answer section 5's question about any app

Version history

VERSION	DATE	CHANGE
1.1	5 September 2026	Founder-voice pass. One honesty-signalling phrase cut. No technical change
1.0	1 September 2026	First release. Describes the position as at the September 2026 case management hearing, with the substantive hearing listed for December 2026