The OSA Is an Invasion of Privacy: What the Online Safety Act Really Means for Ordinary People

10 December 2025

The UK's Online Safety Act (OSA) has been sold to the public as legislation to "keep children safe" and "clean up social media." But the deeper you look into the wording of the Act, the clearer it becomes that this is not a narrow safety measure at all, it is a sweeping restructuring of digital regulation that quietly reaches into **private communication, personal cloud backups, encrypted services, and even self-hosted systems.**

The Act is drafted so broadly that *anything* allowing file upload is treated as if it is a social media platform. That includes cloud services used only by one person, and yes, even private self-hosted cloud servers can fall within scope depending on how Ofcom interprets its powers.

If you want to see the source material yourself, the Online Safety Act is published here on legislation.gov.uk:
https://www.legislation.gov.uk/ukpga/2023/54/contents

Ofcom's regulatory roadmaps and consultations are here:
https://www.ofcom.org.uk/online-safety

This blog post sets out why the OSA is such an aggressive overreach, why privacy experts warn that it fundamentally restructures the relationship between citizen and state, and what it may mean for anyone running a private cloud, including people like me, hosting a personal Nextcloud instance on my own server.

---

1. How the Online Safety Act

Defines Everything as a “Platform”

The first major problem is how the Act defines a **user-to-user service**.

Under the OSA, a platform falls into this category if:

1. A user can upload content, and
2. Another user *could theoretically access it.*

Notice the wording: **could** access, not *does*, not *is intended to*, not *is invited to*.

This means the Act does not require:

- that the content is public
- that sharing is enabled
- that the service is commercial
- that the operator is a business
- or that more than one person actually uses it

By this logic, ordinary cloud storage — Google Drive, iCloud, OneDrive — is treated the same as TikTok or Instagram.

And because the Act contains *no exemption for private self-hosted systems*, even personal services like a home-run Nextcloud technically fall within the definition.

It’s sloppy drafting, and it opens the door to regulatory creep on an unprecedented scale.

---

2. Would Ofcom Really Scan Your Private Files?

Ofcom cannot directly log into your private server. It cannot “scan” your home

cloud from outside. You are not a commercial provider offering a public service.

However, the OSA's structure creates a pathway to something far more concerning:

Client-side scanning

Client-side scanning means:

- Your device scans files *before* encryption
- It happens *before* upload
- It applies to any cloud destination, even your own server
- It turns your phone or computer into the enforcement mechanism

This bypasses the entire question of whether your private server is in scope.

If client-side scanning becomes mandatory for UK users, your device could be forced to inspect:

- personal photos
- family backups
- private documents
- encrypted files

…even if the destination is a completely self-hosted, offline-only, LAN-restricted Nextcloud instance.

This is why cryptographers are unanimous: **client-side scanning breaks privacy entirely.**
It neuters encryption, converts personal devices into surveillance tools, and cannot be safely contained to its original "harm prevention" purpose.

---

3. Plain-English Explanation for Readers: What the OSA Means for You

Here is the simple truth the government will not say out loud:

The OSA treats **private data storage** the same way it treats **public social media**.

If you upload a file into the cloud, even a private backup no one else will ever see, it is now a "regulated activity."

That means Ofcom is positioning itself to oversee:

- cloud storage
- file sharing
- private uploads
- encrypted communication

This was never communicated clearly to the public. Instead, the Act is being expanded step by step through quiet regulatory updates, each drifting slightly further into private digital space.

And once a system like client-side scanning exists, it will inevitably be repurposed. Today the justification is child protection; tomorrow it can be copyright, extremism, misinformation, political content, or **anything the *regulator* decides.**

There is no version of this that stays limited. History is crystal clear about what happens once surveillance capability exists.

---

4. Arguments Against Client-Side Scanning (Feel Free to Use on X)

- If every private file must be scanned “just in case,” then the presumption of innocence has been abolished.
- No democracy should normalise technology that treats every citizen as a suspect.
- Breaking encryption to fight crime is like banning curtains to fight burglary.
- Once client-side scanning exists, governments *will* repurpose it. They always do.
- A device that scans your files for the state is not your device anymore.
- You don’t protect privacy by building a system designed to destroy it.
- Parliament never debated scanning private cloud backups, yet here it is, creeping in through regulation.
- Even if you trust today’s government, you have no control over who inherits this system tomorrow.

These arguments resonate because they’re based on principle, not partisanship.

---

5. Practical Steps to Keep Your Private Cloud Private

Here is a realistic mitigation strategy for people running private servers like Nextcloud.

5.1 Avoid cloud sync apps that could be

forced to include scanning

If client-side scanning becomes law, major vendors (Apple, Google, Microsoft) will comply.

Linux and Free and Open-Source Software (FOSS) ecosystems are harder to force.

5.2 Use Nextcloud through browser access or rsync instead of the sync client

Browser access and manual file transfers avoid the risk of future scanning hooks in sync apps.

5.3 Disable sharing features on your Nextcloud instance

You can disable:

- public link sharing
- user-to-user sharing
- federation
- guest accounts

This reduces any argument that your system is a “platform.”

5.4 Keep Nextcloud local-only (optional but strong)

If you only need access inside your home network:

- Keep it behind NAT
- No public domain
- Access via LAN only

This effectively removes it from the regulatory ecosystem.

5.5 For remote access, use VPN tunnels

WireGuard, Tailscale, or Zerotier keeps your cloud private without requiring public-facing ports.

5.6 Maintain an offshore mirror (advanced)

If the situation escalates, you can run a second copy of your cloud in a jurisdiction that respects privacy.

This is already standard practice for journalists, NGOs, and researchers.

Conclusion: The OSA Goes Far Beyond "Safety" — It Redefines Privacy in the UK

The Online Safety Act has been presented as a child-protection measure, but its wording and Ofcom's emerging guidance reveal something far more intrusive.

A law that treats private backups as regulated content is not safety legislation.
A law that encourages scanning of personal devices before encryption is not proportionate.
A law that quietly expands its scope without public scrutiny is not honest.

This shift needs public pressure, technical expertise, and political challenge — because once client-side scanning becomes normalised, privacy in the UK will not recover.