LIBERTAS
CHAMBERS

clerks@libertaschambers.com | www.libertaschambers.com

The 'Fediverse' vs P2P: The next generation of digital forensics

By Benjamin Knight

The courts of England and Wales may still be dealing with the many EncroChat-related prosecutions, but technology has already moved on. While many are focused on AI and its potential for misuse, what some overlook are the networks on which these platforms operate. You may never have heard of the 'fediverse' but, if you practise criminal law, you should understand the basics.

What is the 'fediverse'?

The fediverse refers to a decentralised social networking architecture. Instead of one company controlling everything, it's made up of thousands of independently operated servers across the internet. These servers can 'federate' by connecting to each other using shared communication protocols. This allows users on different servers to interact, similar to emailing between Gmail and Outlook.

A protocol is a set of rules and standards that devices use to communicate. Servers set their own rules, and if one server goes offline, the others keep working. So there is no central point of failure.

Have I used the fediverse without realising?

If you joined the Twitter alternative Mastodon, you have used the fediverse. Mastodon has no single website – users join independently operated servers, which can all interact as part of the federated network. This confused many accustomed to centralised networks like Facebook or Twitter.

How does it differ from Peer-to-Peer?

The fediverse architecture is similar to peer-to-peer (P2P) networks like BitTorrent, where user devices connect directly without central servers. A server is a powerful computer that provides services to other computers over a network.

However, fediverse platforms focus on persistent social networking via servers that retain identities and relationships over time. P2P apps like BitTorrent emphasise ephemeral, anonymous file transfers between devices instead.

The main P2P messaging apps to be aware of are:

- Briar, Tox, Bitmessage, Ricochet – Decentralised and serverless
- Signal - Uses a decentralised service architecture
- Session - Decentralised with onion routing, doesn't federate
- Matrix - Can bridge to fediverse, but supports non-federated P2P modes

Intercepting P2P networks is difficult without endpoint access. An endpoint is a user device like a phone or laptop. The decentralisation of P2P hinders content decryption without direct endpoint access, especially with proper implementations.

How was EncroChat accessed?

EncroChat used centralised servers, not P2P. In 2020, agencies infiltrated EncroChat by installing tools on their servers to intercept encrypted messages pre-encryption. It appears that different tactics were used by various agencies to harvest data from the EncroChat servers.

There are complex cross-jurisdictional issues around the admissibility of such intercepted material when obtained through infiltration rather than mutual legal assistance processes.

EncroChat shut down their network after discovering the compromise. Their centralised structure enabled network-wide monitoring.

Challenges for legal professionals

The distributed fediverse creates hurdles like:

- No central entity for data requests – servers are worldwide
- Encryption can prevent access even with warrants
- Anonymity and hidden servers hinder investigations
- Inconsistent data retention as policies vary
- Gaps as laws fail to address decentralised networks

Fediverse technologies to be aware of

There are several open-source technologies that make up the fediverse ecosystem:

- Mastodon: Twitter alternative used to share posts and messages
- PeerTube: YouTube alternative for hosting and sharing videos
- Funkwhale: For listening to and sharing audio files and music
- PixelFed: Instagram alternative focused on photo sharing
- Friendica : Facebook alternative that can integrate different social features

Many of these use ActivityPub as the underlying federation protocol. ActivityPub enables sharing and interacting with content across the different platforms.

Encryption in the fediverse

Most fediverse platforms use HTTPS encryption to secure connections between servers and clients. However, end-to-end encryption for messages and content sharing is not yet widespread. Matrix bridges provide one pathway to more private messaging within the fediverse.

Matrix bridges

Matrix bridges allow Matrix users (see above) to communicate with users on other platforms by bridging the different protocols. This provides a way for Matrix users to access and participate in the broader fediverse while still using the end-to-end encrypted messaging capabilities native to Matrix. They work by translating messages between Matrix (which uses its own protocol) and other platforms like Mastodon or IRC. This lets Matrix users message and share content with users on those third-party networks. Matrix clients (apps) implement end-to-end encryption between users even when bridging networks.

The problem with Matrix bridges

Matrix bridges introduce potential risks and vulnerabilities that could be exploited for surveillance. Users should be aware that bridges reside on servers operated by individuals or entities, like any other server software. There is no inherent verification of bridge operators so anyone can create a malicious bridge intended to intercept, monitor or alter communications between Matrix and other networks.

As happened with EncroChat, state actors could potentially run bridges embedded with "malware" to surveil users. Even legitimate-looking bridges could be compromised and backdoored without users' knowledge.

Metadata and even message contents could be quietly collected from users of a malicious bridge. Keys for end-to-end encrypted conversations could be stolen through a compromised bridge.

Matrix bridges extend the encrypted messaging capabilities of Matrix into the fediverse, they do effectively introduce third-party relay points that could be abused for surveillance.

Adapting investigations

Law enforcement agencies will likely need to quickly adapt strategies and capabilities to investigate criminal activities within decentralised fediverse platforms. Some approaches agencies may pursue include:

- Developing large-scale traffic analysis tools to map the fediverse and identify potential targets based on communication patterns and metadata. This will rely heavily on artificial intelligence and machine learning capabilities. It is notable that algorithmic analysis (likely a neural net - an AI) was used to trawl the EncroChat data received by multiple state agencies.

- Cultivating cooperative relationships with 'ethical' server operators who can voluntarily provide data to investigations when appropriate legal thresholds are met. However, identifying and vetting reliable partners will be challenging, and those operators will likely be avoided by those seeking to operate covertly for the purposes of illegal activity.

- Establishing lawful intercept capabilities within cooperating jurisdictions to capture unencrypted fediverse traffic traversing internet infrastructure. This will require new international legal frameworks for decentralised networks. The UK is arguably in a weaker position for this since Brexit.

- Exploiting any vulnerabilities found within fediverse protocols, apps, and libraries for decryption and surveillance purposes when technically feasible. This could raise significant ethical and legal questions, however.

- Using legal warrants and court orders to compel identified users or server operators to provide decrypted data or encryption keys. But jurisdictional reach will be limited. Again, in the EncroChat litigation of most affected countries, the fact that the platform was believed to be used almost exclusively for criminal activity was used as justification for allowing highly invasive methods to be used. It is likely that care will be taken by "the next EncroChat" architects to avoid creating a system so easily isolatable as a 'criminal network'.

- Running undercover sting operations directly within federated platforms for evidence gathering. But maintaining cover will be difficult long-term. It is surprising that previous such activities stayed secret for as long as they did.

- Shaping policy and legislation proactively to mandate lawful access provisions and prevent criminal exploit. However, proper oversight is necessary to prevent overreach.

Navigating this new terrain will require updated strategies, greater technical capabilities, and increased global cooperation between investigative agencies. But the challenges of decentralised networks can be managed through preparation and striking the right balance between safety and ethical practices.

Preparatory steps for lawyers

When fediverse platforms or data are identified in an investigation, solicitors and barristers should move quickly to gather key information that may be volatile or at risk of loss in these decentralised ecosystems. That involves very swift liaison with the police and engaging with the DMD protocol. It is more likely that the police/NCA will have quicker access to this information than defence solicitors. Assuming instructions from the lay client are such that obtaining as much related data as possible is desirable, sending formal requests for these actions is prudent.

The following information should be requested at the earliest stage (often pre-charge). When the information is obtained, it will enable an expert to provide more confident conclusions if/when instructed.

It would be sensible to start by identifying the specific servers and accounts involved, as data may be siloed across multiple jurisdictions. Sending preservation requests to each server's operator may prevent deletion. Obtaining user lists, message logs, content snapshots, and traffic/usage statistics should be prioritised while available. Even if that information is not provided immediately, asking the operator to secure it is a sensible place to start.

Ask the investigators to probe the protocols and software versions used by each server to understand technical capabilities and vulnerabilities. Ask them to request server policies on areas like encryption, anonymity, and moderation, and ask if end-to-end encrypted channels are implemented.

Learn whether the servers retain message content or mainly transactional metadata. Ask what data is logged, how it is secured, and how long it is kept.

Look for information on the owners, operators, and user base of each server. This can aid jurisdictional determinations and provide leads for further investigation, if required.

Solicitors and barristers should try to stay up-to-date on which platforms and apps see growing usage in criminal contexts like drug trafficking, explosives trafficking, extremism, money laundering, and child exploitation. Mastodon, PeerTube, Matrix, and Jabber are increasingly common, although legitimate applications such as Zoom, WhatsApp, and Facebook Messenger are in common usage for illegal activity.

Although very old now, basic web chat platforms such as Omegle and TinyChat appear with alarming frequency in IIoC cases, even in 2023.

Training

Given the complexity of these systems, engage technical experts early on to advise on evidence gathering, analysis, and prevention. Online offences and core IT knowledge training will become increasingly valuable for experts, investigators, and legal professionals. Staying on top of the basics of evolving technology will make individual cases easier to follow and will assist even in the police station stage.