A Specification for Encrypted Safe Spaces.

The basis for this specification for Secure Safe Spaces came from a POC developed for Diversity-Live a non-profit organization hoping to become the first of a new kind of crowd funded organization for monitoring, cataloging and responding to abuse of Marginalized groups in the United states.
Diversity-Live's infrastructure will be centered around a newer version of our jointly developed RIMS System, Rapid Incident Monitoring , the new infrastructure is called Super Mesh.

Privacy is almost an oxymoron in todays connected society, you write a blog post or a tweet and after hitting send you have little control over what happens to that post.

It can be read by the public or if it's in a private group restricted only to your friends. But that post is also visible to the support personal at the social media company.

Hidden inside long hardly readable Terms of Service agreements are implied contracts that let these companies share all kind of personal information with third parties.
This information, a little slice of your life could be used for targeted adds, sold to third party analytic companies to determine anything from what toothpaste brand are you likely to buy to what political candidate you may favor in the next election.

People want privacy, but the meaning of “Privacy” is sometime forgotten these days.

Let's say you respond to a post inviting participation in a rally for Women's rights.
You view the post sign up tentatively for the event but never actually attend.
Violence breaks out at the event and the DOJ requests the records of everyone that so much as visited the event post.

This occurred after isolated violence erupted at an anti-Trump rally at the time of the Presidents inauguration the admin wanted the personal info from over 6,000 visitors to the site organizing the rally. If you think this is unconstitutional, violation of free speech the court did grant limited access to some of the protestor's information.

This is should clearly be unconstitutional but if you have one party that has stacked the judiciary with biased judges it can and does happen all to frequently.

Ideally you want to make it difficult for the social media company to turn over your private information which may include personal information, photos of you and your family etc.

Encryption may sound like the ultimate remedy, with an authoritarian like government to assure some sense of privacy, including protection from false incrimination by a paranoid administration.

But in Developing the Encrypted Safe Spaces specification we had to also address the possibility of bad “actors” or terrorist using these encrypted spaces for plotting their next attack.

Law enforcement will try to make the case that the social media provider was aiding and abetting terrorist and that they must be given back door access to all posts even encrypted ones.

The challenge is to provide a method that insures the social media site does not have the decryption key, if law enforcement wants access to the decrypted content, they must go back to the owner of the posting account. Issuing a Subpoena to the social media company is pointless because they have no way of decrypting the private information.
At the same time the system must be able to survive such court challenges.

For Encrypted Safe spaces we came up with something called a litigation work flow which would provide satisfactory proof to authorities that the post did not contain information relating to terrorism, national security, child pornography etc.

So, what does an encrypted safe space look like from 10,000 feet.

We start with a post or a series of post associated with a user’s account.
This post may already be shared with several other users.

The owner of the blog using an authenticated device requests that the posts be encrypted.

This causes a series of events.

First a copy of the post is created and encrypted, a unique decryption key is generated
And sent to the account users’ device.
Only the owner has access to the first generation copy of the post via her unique encryption key stored in a secure KeyStore on her device.

A second generation copy of the post is made from the original unencrypted post and a temporary decryption key is generated. this key is now distributed to all authorized sharers of the   post. Once generated this key is sent to the authorized devices owned by the followers and stored in secure KeyStore on their devices.

There is a cloud KeyStore specification in the specification, but the use of external devices assures the decryption key is never present on the server.

An authorized follower wishing to read the posts for a specific encrypted safe space must authenticate with their registered device, once authenticated the decryption key is retrieved from the KeyStore and used to decrypt the second generation copy of the post.

Only users with the decryption key may read the posts. The first-generation encrypted copy of the posts may only be accessed by the account owner and only for the purpose of re-encryption after a key regeneration, which may occur if a follower is removed from the group because of abuse.
The original post is permanently deleted after being encrypted.
Otherwise old posts are retrieved using the original second-generation key and newer posts are only available to remaining followers with the new key, both keys would be stored in the encrypted keyStore.

In the event of an abusive removal, the account owner would decrypt the first generation copy of the post with her first-generation key, create a new second generation copy of the post and distribute the keys to the remaining authorized devices. The unencrypted posts are always permanently deleted.

These copy/key generations and distribution are transparent to the users due to the design of super mess architecture which is built around hardware encryption. Other cloud-based implementations of the spec performance will vary based on Hardware.

Other generational copies could be made with expiring keys, these could be temporarily made available to law enforcement at the owner's request.

An enhanced version of the specification does include videos, but the workflow is different and not publicly available yet.

Litigation Workflow

We mentioned that encrypted safe spaces must be able to survive any court cases that attempted to limit them due to false claims of National Security threat or accusation that the system was developed to aid criminals.

The concept is brilliantly simple.

When the account holder makes a request to encrypt a post or series of post and include them in a secure safe space. The request must be reviewed.

Unfortunately for now this can be a somewhat slow process because the request must be processed by a human. As ML algorithms get better it's entirely possible some of the review process could be automated.

Corporate sites trusted accounts and those around incidents of abuse could under some circumstances bypass the review process.

But the normal process is a review is made of the posts to be encrypted, the owner signs an affidavit indicating that the posts do not contain information about contraband, terrorist's info, pornography, a whole list of prohibited activities.
This affidavit is electronically signed and sent to the reviewer, the reviewer than views the contents of the site, makes notes about content on the affidavit, electronically signs it. and the affidavit is stored unencrypted with the safe space.

If there is ever any questioning by law enforcement, they are sent whatever information they are "entitled" too depending on the request or Subpoena if that includes owner information than they must go back to the original owner to gain access to the contents of the safe space. Law enforcement is also presented with the signed affidavits associated with the encrypted material.

That is a brief very high-level overview of encrypted Safe Spaces.