Section 1: Parts of the Draft that People Seem Fine With
Basic Model

1. **Search**: What’s the value of this key?
2. **Update**: Here’s a new value for this key!
3. **Monitor**: What’s new with my keys?

- Looks like a key-value database
- Transparency Log enforces access control rules by simply rejecting queries that aren’t allowed
- User (generally) only needs direct communication with the Transparency Log
### Deployment Modes

<table>
<thead>
<tr>
<th>Name</th>
<th>Applications that Generally Follow this Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Monitoring</td>
<td>Google KT, Apple iMessage KT</td>
</tr>
<tr>
<td>Third-party Auditing</td>
<td>WhatsApp KT</td>
</tr>
<tr>
<td>Third-party Management</td>
<td>Certificate Transparency, Merkle Tree Certificates</td>
</tr>
</tbody>
</table>

Supports a wide range of use-cases
1. Contact Monitoring

```
User

What's Alice's public key?

Here it is, with proof!

That version of Alice's public key that you showed me is still in the database right?

Yep it's still there, here's proof!

...```

Transparency Log
2. Third-party Auditing

Many users

Transparency Log

Third-party Auditor

Here’s a list of all the changes I made to the database today!

Looks like you did everything right, here’s a signature saying that
3. Third-party Management

User → Transparency Log → Third-party Manager

I’m Alice, here’s my new public key

Here’s Alice’s new public key

I updated her key, here’s proof

Here’s proof your key was updated
Out-of-Band Communication

Peer-to-Peer Gossip:
- Manual, low bandwidth
- Envisioned as users scanning QR codes

Anonymous Channel:
- Automated!
- Envisioned as fetching a tree head over an anonymous network

- **Important Point #1:**
  Out-of-band communication is always about tree heads, and never individual users

- **Important Point #2:**
  Gossiping effectively requires having a linearizable view (next slide!)
“Linearizable View”

- Users remember the most recent tree head they’ve observed and require future queries to be provably consistent against that tree head
- **Implies:** At minimum, a constant-size amount of state
- **Benefit:**
  - Makes out-of-band communication much more effective
  - In third-party auditing: Allows immediate updates despite auditor lag

(We’ll discuss this more later)
(Intermission)
Section 2:
Feedback from the Mailing List
Missing Sections

- Support for Sealed Sender

- Discussion of how federation would work

- Discussion on privacy law compliance / compelled deletion of user data
Immediate Updates?

- Currently the draft states that requested changes are applied **immediately**

- **Implies:** No ‘interim’ inclusion proofs (similar to SCTs)

- **Benefits:**
  - Simplifies protocol description and operation
  - Supports deployments that want a ‘strict’ KT regimen

- Deployments that don’t trust their KT server’s reliability / performance seem to have sufficient other risk-reduction strategies
Questions?
Thoughts?