

Privacy Primer for vCon Developers

Thomas McCarthy-Howe, *CTO*, Strolid

Diana James, *Attorney, CIPP/US*, The CommLaw Group

Protected Data Within Vcons

- Personally identifiable data
 - Names (parties)
 - Biometrics (voiceprints)
 - Protected characteristics (analysis)
 - Financial data (dialogues)
 - Etc.
- Communications data
 - The conversation's content (transcripts and recordings)

Unprotected Data

- Deidentified data (data from which identifying information is removed)
 - information suppression (direct removal of information)
 - generalization (replacing a data element with a more general equivalent)
 - noise addition (adding carefully calibrated noise to the data)
 - Anonymization is the ultimate and irreversible type of deidentification
- Aggregated data (summarized data from multiple sources, with identifying data removed from final product)

• Re-identification risks must be mitigated

vCon offers a straightforward way to redact personally identifiable information by:

a. PII masking or

b. Removing segments or whole recordings

Privacy Principles (1/3)

1. Notice/Transparency

2. Consent

- vCon allows storage of consent data, tracking permissions for specific data uses.

3. Purpose, Collection, and Storage Limitation and Data Minimization

- vCon permits masking and deletion of personally identifiable information, which reduces the amount of data processed and stored in accordance with this principle.

Privacy Principles (2/3)

4. Security

- Vcons can and in some cases should be encrypted.
- Externally referenced files that are part of a vCon should be encrypted if they contain protected information and should be transported only over HTTPS.
- Access to unredacted vCons and their referenced files should be restricted to authorized personnel only.

5. Data Integrity

- vCon can be used with SCITT to track conversational data's provenance and ensure its integrity.

6. Recordkeeping

- Ability to keep the call's contents, metadata, and attachments in a single "container" makes vCons useful for industries with strict record-keeping requirements (e.g., financial services and healthcare).

Privacy Principles (3/3)

7. Individual Rights

- Right of access
- Data choices:
 - “right to be forgotten”
 - right to data portability
 - right to opt out of certain data practices
 - right to data breach notification
- vCon helps quickly find what data is associated with a particular person to act on consumer data choices or notify of data breaches.
- vCon + SCITT can help notify other data processors of consumer’s choices.

Conclusion

- vCon is not a silver bullet for privacy compliance but can help those willing to comply.
- vCon's compliance effectiveness can be enhanced by using other compatible protocols, such as SCITT, with it.