Is federated learning (FL) safe?

Gradient carries information in the training data.

- Least squares regression:

$$\min_{\mathbf{w}} \sum_{i=1}^{n} l(\mathbf{w}, \mathbf{x}_i, y_i), \quad \text{where } l(\mathbf{w}, \mathbf{x}_i, y_i) = \frac{1}{2}\left(\mathbf{x}_i^T \mathbf{w} - y_i\right)^2 .$$

- Stochastic gradient:

$$\mathbf{g}_i = \frac{\partial\, l(\mathbf{w}, \mathbf{x}_i, y_i)}{\partial\, \mathbf{w}} = \left(\mathbf{x}_i^T \mathbf{w} - y_i\right) \mathbf{x}_i .$$