Privacy and End-to-End Encryption

Embedded Ethics Lecture

Veronica A. Rivera, PhD
varivera@stanford.edu
Today:

Encryption can be used to protect privacy

If we use it well
Privacy in the digital age refers to...
Private messaging is important for daily life
Encryption

\[ c \leftarrow \text{Enc}(k, m) \]

\[ m \leftarrow \text{Dec}(k, c_k) \]
No Encryption (FB 2010)
Transport Layer Security (TLS) (FB 2012): Encryption between clients & servers
End-to-End Encryption

\[ c_{k_{A,B}} \leftarrow Enc(k_{A,B}, m) \]

\[ m \leftarrow Dec(k_{A,B}, c_{k_{A,B}}) \]
E2EE does not solve all privacy problems

• Need to get random people to agree on shared keys
• Metadata (call logs, phone number, location) isn’t hidden and could still be collected
• Content moderation becomes very hard to solve because platform can’t read content
• Ends (e.g., phones) are still vulnerable