

# Off The Record messaging

A gentle introduction

London CryptoFestival 2013

# Why bother?

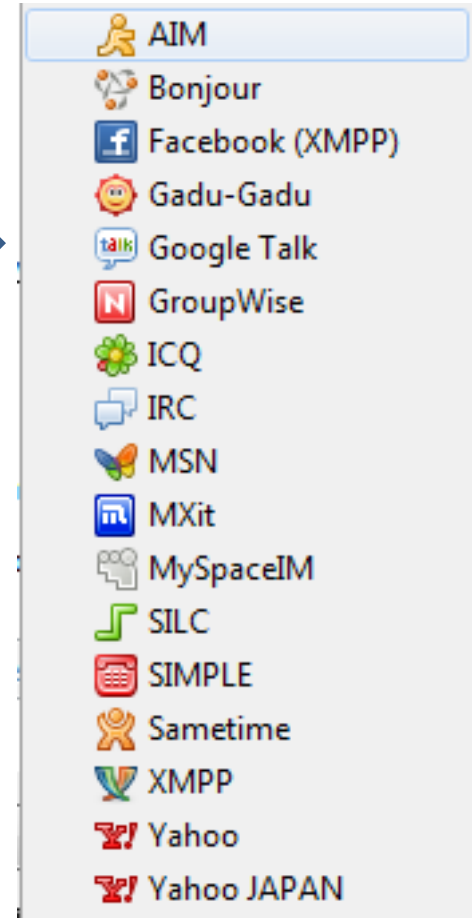
- Casually chatting ON the record is dangerous
- Casual = you will say something that can be used against you
- Perhaps 30 years from now.
- Hey, it's all recorded and you can't delete the record. You can't even see your record!

# But I can delete my chat history!

- No you can't.
- All you can do is *stop seeing the record*
  - Google's "Go off the record" => STILL RECORDED!
  - Facebook's "Delete" => DOESN'T DELETE!
- But I have rights to my data as an EU citizen!
  - In theory, you should be able to get a copy of your data.
  - Good luck with that - see "Europe vs Facebook"  
<http://europe-v-facebook.org/EN/en.html>

# But all my friends are on...

- No need to change your current chatting/social network – most are supported
- Off The Record (OTR) messaging
  - Privacy over public channels
  - Use Google chat without Google reading what you say!



# What OTR gives you

- **Encryption**
  - No one else can read your instant messages.
- **Authentication**
  - You are assured the correspondent is who you think it is.
- **Deniability**
  - The messages you send do *not* have digital signatures that are checkable by a third party.
  - Anyone can forge messages after a conversation to make them look like they came from you.
  - *During* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- **Perfect forward secrecy**
  - If you lose control of your private keys, no previous conversation is compromised.

# Best OTR tools

-  with pidgin-otr on Windows

<http://pidgin.im/> and <https://otr.cypherpunks.ca/>

- ChatSecure on Android & iOS

<https://guardianproject.info/howto/chatsecurely/>

-  Adium on Mac <https://www.adium.im/>

-  CryptoCat on anything! <https://crypto.cat>

# Key verification

- Verifying your correspondent ensures there is no “Man In The Middle” (i.e. eavesdropper)
- Video tutorial: <https://www.youtube.com/watch?v=vgx7VSrDGjk>
- You only need to do it once!
  - for each correspondent

# What encryption looks like

You say "hello" over OTR

cryptoparty2013@jabber.ccc.de

(08:11:07) cryptoparty2013@jabber.ccc.de has not been authenticated yet. You should authenticate this buddy.

(08:11:08) Unverified conversation with cryptoparty2013@jabber.ccc.de started.

(08:12:30) The privacy status of the current conversation is now: Private

(08:12:54) cryptoparty2013@jabber.ccc.de **hello**

cryptoparty2013 says... - Mozilla Firefox

cryptoparty2013 says...

https://mail.google.com/mail/?shva=

Google

Gmail

COMPOSE

Primary

Inbox

Starred

Important

Sent Mail

Search people...

cryptoparty2013

Alex Leme

0 GB (0%) of 15 GB used

Manage

©2013 Google

cryptoparty2013

gFyOJDHb1nLCbeC  
mpVYjKPvumiM8G6  
hTr2510ooVPw3lj  
YS01AIPt25O1OcL  
MAPYIC7v0cJbwL  
U4ZWogk4ELZYQAA  
AAAAAABAAAAABR7  
vdoABgXMeXrNWbO  
07I3q8t110xYZF/  
0cAAAAUt2R763WY  
Tw6GHY52k1niMhzmDx8=.

Sent at 8:12 AM on Saturday

Press Enter to send your message.

This is what Google sees!



Demo time!

# Questions?

- Step-by-step instructions:
  - Using OTR with Facebook:  
<http://apapadop.wordpress.com/2012/03/29/stop-facebook-recording-your-chats/>
  - Using OTR with Google Chat:  
<http://apapadop.wordpress.com/2012/04/15/stop-google-recording-your-chats/>