Tor

- Anonymized internet access so websites don’t know where you are
  - Great for research so websites don’t know you visited them & your ISP doesn’t know either.
- Relays your web traffic through random computers before trying to access the website
- Caveats:
  - Slower than normal browsing
  - Relays may see your browsing (if not HTTPS), since they are relaying it on behalf of you. (Be careful with logins!)

Tor

PC/Mac: https://www.torproject.org/

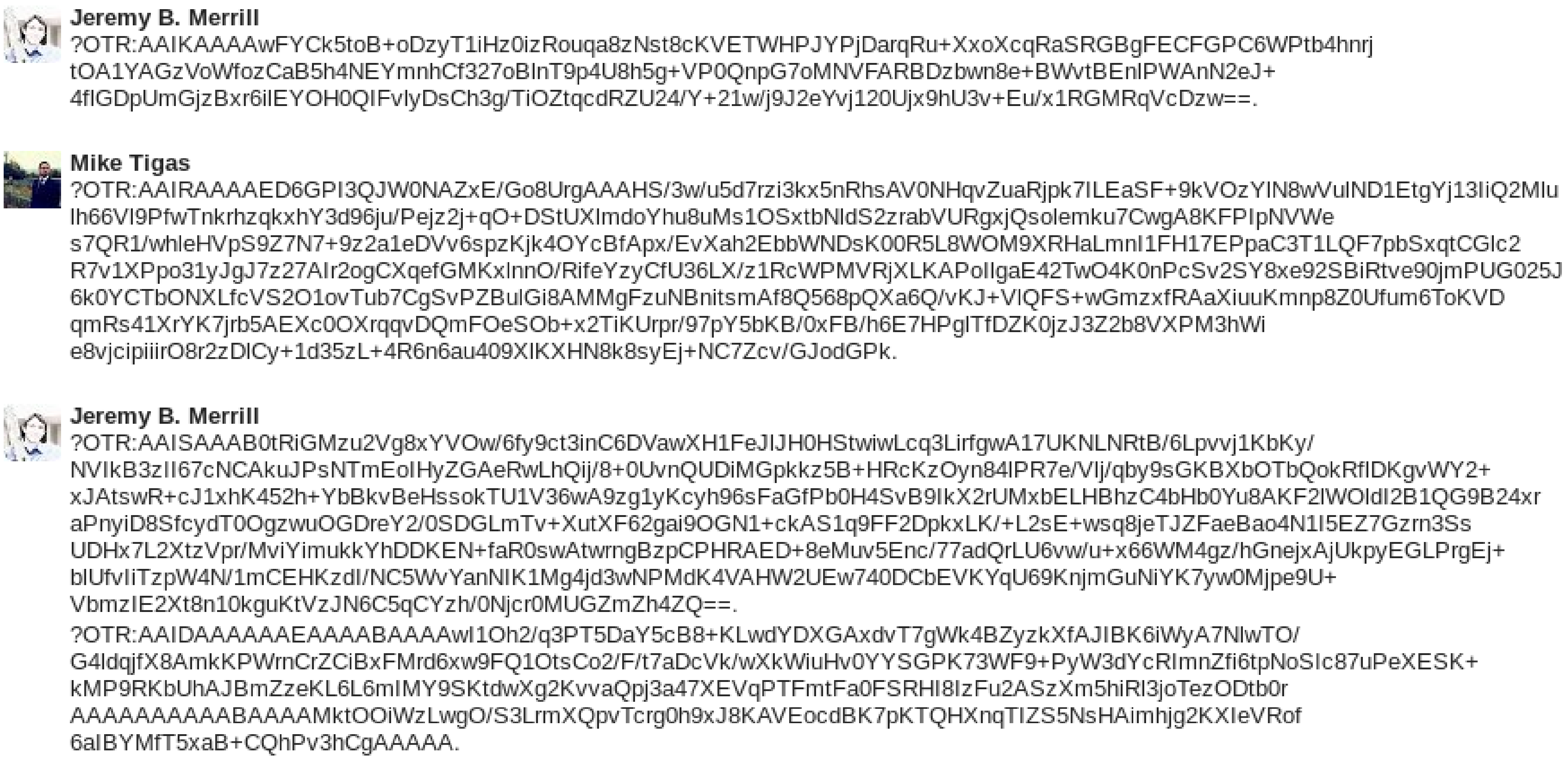
iOS: Onion Browser (disclosure: I work on this)

Android: Orbot

Chat: OTR Encryption

- “Off The Record” encryption protects messages between you and someone else.
  - Not the same as Google “Off The Record” mode
- Use an existing account (like GChat or others) & use an OTR plugin to encrypt.
  - You can register an account at other chat services too, to avoid Google knowing about your chats.
- Caveats:
  - Metadata – who you are talking to and when – is still seen by the chat service.

OTR Encryption



Jeremy B. Merrill

?OTR:AAIKAAAAwFYCk5toB+oDzyT1iHz0izRouqa8zNst8cKVETWHPJYPjDarqRu+XxoXcqRaSRGBgFECFGPC6WPtb4hnrj
tOA1YAGzVoWfozCaB5h4NEYmnhCf327oBlnT9p4U8h5g+VP0QnpG7oMNVFARBDzbwn8e+BWvtBEnlPWAnN2eJ+
4flGDpUmGjzBxr6ilEYOH0QIFvlyDsCh3g/TiOZtqcdRZU24/Y+21w/j9J2eYvj120Ujx9hU3v+Eu/x1RGMRqVcDzw==.

Mike Tigas

?OTR:AAIRAAAAED6GPI3QJW0NAZxE/Go8UrgAAAHS/3w/u5d7rzi3kx5nRhsAV0NHqvZuaRjpk7ILEaSF+9kVOzYIN8wVulND1EtgYj13IiQ2Mlu
lh66Vl9PfwTnkrhzqkxhY3d96ju/Pejz2j+qO+DStUXlmdoYhu8uMs1OSxtbNldS2zrabVURgxjQsolemku7CwgA8KFPIpNVWe
s7QR1/whleHVpS9Z7N7+9z2a1eDVv6spzKjk4OYcBfApx/EvXah2EbbWNDsK00R5L8WOM9XRHaLmnl1FH17EPpaC3T1LQF7pbSxqtCGlc2
R7v1XPpo31yJgJ7z27Alr2ogCXqefGMKxlnnO/RifeYzyCfU36LX/z1RcWPMVRjXLKAPollgaE42TwO4K0nPcSv2SY8xe92SBiRtve90jmPUG025J
6k0YCTbONXLfcVS2O1ovTub7CgSvPZBulGi8AMMgFzuNBnitsmAf8Q568pQXa6Q/vKJ+VlQFS+wGmzxfRAaXiuuKmnp8Z0Ufum6ToKVD
qmRs41XrYK7jrb5AEXc0OXrqqvDQmFOeSOb+x2TiKUrpr/97pY5bKB/0xFB/h6E7HPglTfDZK0jzJ3Z2b8VXPM3hWi
e8vjcipiiirO8r2zDlCy+1d35zL+4R6n6au409XlKXHN8k8syEj+NC7Zcv/GJodGPk.

Jeremy B. Merrill

?OTR:AAISAAAB0tRiGMzu2Vg8xYVOw/6fy9ct3inC6DVawXH1FeJIJH0HStwiwLcq3LirfgwA17UKNLNRtB/6Lpvvj1KbKy/
NVIkB3zII67cNCAkuJPsNTmEoIHyZGAeRwLhQij/8+0UvnQUDiMGpkkz5B+HRcKzOyn84lPR7e/VIj/qby9sGKBXbOTbQokRfIDKgvWY2+
xJAtswR+cJ1xhK452h+YbBkvBeHssokTU1V36wA9zg1yKcyh96sFaGfPb0H4SvB9IkX2rUMxbELHBhzC4bHb0Yu8AKF2lWOldI2B1QG9B24xr
aPnyiD8SfcydT0OgzwuOGDreY2/0SDGLmTv+XutXF62gai9OGN1+ckAS1q9FF2DpkxLK/+L2sE+wsq8jeTJZFaeBao4N1I5EZ7Gzrn3Ss
UDHx7L2XtzVpr/MviYimukkYhDDKEN+faR0swAtwrngBzpCPHRAED+8eMuv5Enc/77adQrLU6vw/u+x66WM4gz/hGnejxAjUkpyEGLPrgEj+
blUfvIiTzpW4N/1mCEHKzdI/NC5WvYanNIK1Mg4jd3wNPMdK4VAHW2UEw740DCbEVKYqU69KnjmGuNiYK7yw0Mjpe9U+
VbmzIE2Xt8n10kguKtVzJN6C5qCYzh/0Njcr0MUGZmZh4ZQ==.

?OTR:AAIDAAAAAAEAAAABAAAAwI1Oh2/q3PT5DaY5cB8+KLwdYDXGAxdvT7gWk4BZyzkXfAJIBK6iWyA7NlwTO/
G4ldqjfX8AmkKPWrnCrZCiBxFMrd6xw9FQ1OtsCo2/F/t7aDcVk/wXkWiuHv0YYSGPK73WF9+PyW3dYcRImnZfi6tpNoSlc87uPeXESK+
kMP9RKbUhAJBmZzeKL6L6mIMY9SKtdwXg2KvvaQpj3a47XEVqPTFmtFa0FSRHI8IzFu2ASzXm5hiRI3joTezODtb0r
AAAAAAAAAABAAAAMktOOiWzLwgO/S3LrmXQpvTcrg0h9xJ8KAVEocdBK7pKTQHXnqTIZS5NsHAimhjg2KXIeVRof
6aIBYMfT5xaB+CQhPv3hCgAAAAA.

OTR Encryption

- Tor Messenger provides OTR encryption and lets you use accounts on many messaging services (Google Chat, Twitter DMs, XMPP/Jabber).
  - In addition to OTR, it uses Tor to mask your IP address.
- ChatSecure is similar, but for iPhone and Android.

Remember: to use OTR, your friend also needs to use Tor Messenger (or another app that does it).

Encrypted Texts

- Signal (iOS & Android)
- iMessage (iOS) claims to encrypt messages, but Apple may have access to the messages.
  - Phone provider doesn't se messages anymore, but Apple has the metadata of who you communicate with.

Phone Calls

- Signal (iOS & Android)
- SilentCircle ($$$, iOS & Android)
- FaceTime (iOS): Like iMessage.
  - Prevents cell provider from knowing who you call. But again, Apple may have access to the metadata and actual call.

PGP

Also known as GPG — for “GnuPG”, one of the programs that does this

Public and private keys, you have to know someone's public key to send them an encrypted message.

Also lets you “sign” messages so recipient can tell whether it was tampered with while in transit.

PGP

- Mac:
  Thunderbird+ Enigmail
  or GPGTools + Mail app
- Windows:
  Thunderbird+ Enigmail
  or GPG4Win + Outlook
- Setup guides:
  Hacks/Hackers NYC
  Freedom of the Press Foundation
  Security in a Box

But what about other tools?

- New tools come out all the time.
- We don’t necessarily know what’s secure. Follow a lot of security experts to see what their consensus is.
- Consider the encryption, metadata-masking capabilities, and transparency of how tools work:
  - https://projects.propublica.org/graphics/privacy-tools

Further reading

Freedom of the Press Fdn. encryption guide

Threat Modeling guide on OpenNews Source