On Getting In Touch For You With Privacy Concerns

Andreas Michael

*Self Led You*

Last updated: November 4, 2021

**Contents**

1. What This Document Is & Is Not 3

2. Setting Expectations 3

3. On Getting In Touch 4

4. Anonymity via I2P 6
## List Of Changes To This Document

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 September 2021</td>
<td>Initial version</td>
</tr>
<tr>
<td>9 October 2021</td>
<td>Minor changes to text and fixing a broken link to the encryption tool.</td>
</tr>
<tr>
<td>4 November 2021</td>
<td>Minor changes to text and updating DeltaChat contact details</td>
</tr>
</tbody>
</table>
1 What This Document Is & Is Not

It can be difficult to navigate privacy and anonymity when we use so much technology to get in touch with one another. I wrote this document to give you a overview of what you can expect when it comes to privacy and anonymity when working with me. It also describes practical ways of getting in touch with me if you have special privacy needs.

*Please note that this is not a privacy or confidentiality statement.* It’s a practical guide for you who may have particular privacy concerns. For my privacy/confidentiality statement with an overview of the data I (normally) collect through our interactions and what I do with this data, please see my Terms of Service on my website.

2 Setting Expectations

Private From What Or Who?

There is much information out there on online (and in-person) surveillance, data on us stored for an indeterminate amount of time, big data analysis, social credit systems, etc. It’s easy to get overwhelmed. If you have serious privacy concerns, it may be helpful to spend some time to answer questions such as:

- Who, precisely, is watching? (Name a person, organisation or group)
- To what purpose?
- What, in the worst case, is this person or group going to do with this information?
- What, specifically, makes *me* a more likely target for surveillance or special effort from this person or group than my neighbours or others I know?
- What, precisely, is the worst-case impact for me, my life and my loved ones?
- How likely is it that any of this will happen?
- How likely is it to happen to one of my neighbours?
By providing specific answers to these questions, you’ll have a better view of who you are intending to be private from, why, and what practical action can be taken to ensure privacy. In many parts of the world, the answers to these questions will be gloomy indeed, especially if you are not white or are engaged in activities that are challenging the status quo. Together we can understand whether it’s possible for us to design secure ways of effectively communicating to help you with your needs.

On Privacy & Being Anonymous

Privacy: the quality or state of being apart from company or observation

Anonymous: of unknown authorship or origin

Privacy in a conversation with me would mean that the content of our conversations is not overheard. Having a conversation anonymously means that nobody knows who is talking to me.

Depending on your answers to the questions above, you can start thinking about a plan to keep certain information private and/or anonymous and whether you need privacy, anonymity, or both. In general, it is easier to have a private conversation than an anonymous one.

3 On Getting In Touch

General Principles

Like most people, I use many devices & applications. I’ve put considerable effort into making sure that these are privacy-respecting. My general criteria are that software and services I use are federated, open-source and use zero-knowledge encryption on the side of service providers. Any software I need to use that do not fill these criteria, I put in environments that are isolated from the ones I use day-to-day.

With most cloud services (like e-mail, contacts sync, data storage, etc), it’s near-impossible for the layman to determine whether something is truly private or not. If you are not an expert, you can rest assured that your privacy & confidentiality is taken seriously. If you
are an expert, I will leave it to you to determine whether my setup is secure enough for your needs. I am open to suggestions of alternate routes of connecting at your recommendation.

Services & providers I use:

- E-mail: My email is hosted by ProtonMail in Switzerland. If you wish to get in touch with me privately via e-mail, you have options:
  1. Register a free ProtonMail account and use that to e-mail me. ProtonMail will automatically encrypt the message you send. Please note subject lines and email addresses are not encrypted, so put anything private in the message body.
  2. Use my public key (available [HERE] to send me an encrypted email from your email client that supports PGP / GPG e-mail encryption standards (please note subject lines and email addresses are not encrypted). You can also use my public key with the following web page to generate your encrypted message in your web browser and then send your message in any way you wish: [LINK].

- Phone SIM-cards: British Telecom (EE) (British) and Vimla! (Swedish)

- Internet broadband: Virgin Media

- VPN: ProtonVPN

- Contacts & calendar sync: EteSync

- Domain hosting: I Want My Name

- Web hosting: FastMail

- Online scheduling: SquareSpace (Acuity Scheduling) or via e-mail/messaging

- Online video calls: 8x8 (Jitsi), Zoom, Skype

- Accounting: QuickBooks (anonymous for you as I manually clean personally identifiable data before uploading anything into QuickBooks)

- Payments: Cryptocurrency (XMR), BACS (Starling Bank), Stripe, PayPal
• Messaging – needing a phone number: *Signal*, *Telegram*, *WhatsApp*, *text message*

• Messaging – not needing a phone number: *DeltaChat (andreasmjg AT e.email)*, *Briar* *(possible after we establish communication in some other way)*

**Devices I Use & Where:**

• Mobile phone: I use a *OnePlus 5* device running a privacy-respecting operative system called */e/OS* (by e.foundation)

• Laptop: I use a *Lenovo Thinkpad T490s* running Linux (Ubuntu) with firmware-level phone-home features permanently disabled (Absolute’s CompuTrace).

• Primary location: London, England. *(If my physical location matters to you and needs to remain fixed for our conversations, please let me know.)*

**4 Anonymity via I2P**

If you have serious concerns about privacy and especially anonymity, I offer additional ways of getting in touch via the Invisible Internet Project (I2P) Network. I2P is designed to offer both privacy and anonymity. Please note I only check I2P channels about once weekly, sometimes less often.

In order to use these channels, you need to install I2P on your device and can find instructions for how to do that here: [[LINK]].

1. **E-mail:** Set up your email client to use the I2P service on your device. Then send me an email to "andreas@mail.i2p". The email will only arrive if you are connected to the I2P network. You cannot send email from non-I2P email providers to this address.

2. **Messaging:** Setup your IRC client to use the I2P service on your device. Send a private message to "andreas" on the I2P IRC network. Please note I can only respond to you when you are online so if you leave me a message, make sure to also provide a way for me to get back in touch with you.