**1.3 You on the Mobile Network**

**Intro:** Discussion of what makes users uniquely identifiable on the mobile network, and how this information might be misused.

**Timing: 45 minutes-1.5 hours**

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to outline instruction content and participant’s contributions, and to take notes.

**Content Outline and Main Topics:**

1. **Discussion/Instruction (15 - 30 minutes):** SIM registration.
   1. Registration on the network: Registered vs unregistered SIMs
   2. Discussion: Story of your SIM(s). Ask participants how they obtained their SIMs (current and past), and the trade-offs of registered versus unregistered SIMs where they live and work.
2. **Instruction (15 - 30 minutes):** Intro to identity on mobile networks.
   1. MNO subscriber records (*who they think you are*)
   2. Unique identifiers (*what you look like to an MNO*)
   3. Geolocation (*where you are*)
   4. Data logging by MNOs (*what they collect and store)*
3. **Instruction (15 - 30 minutes):** Issues of identity.
   1. How to be anonymous on mobile networks
   2. How the identity of an anonymous user might be discovered
   3. Unlocked/jailbroken/rooted devices
4. **Summary and Action Items**

**Objectives/Expected Outcomes:**

* Participants will learn the central elements that make them uniquely identifiable as mobile phone users and how obscuring your identity can be used as a tactic.
* Participants will gain basic awareness of other issues affecting privacy/identity.

**Additional Resources:**

[Mobile Risk Assessment](http://mobileactive.org/howtos/guide-mobile-risk-assessment)

[Mobile Security Risks: A Primer](http://www.mobileactive.org/howtos/mobile-security-risks)

<http://www.mobileactive.org/howtos/mobile-security-risks>

**Content**

**1. Discussion/Instruction (15 - 30 minutes):** SIM registration.

1a. **Registration on the Network:** Registered vs unregistered SIMs

* **Registered SIM:** A registered SIM requires users to provide identification for activation. In Nigeria, for instance, this includes fingerprints and photos, as well as proof of address. All contract SIMs are effectively registered SIMs, because the MNO has a record of your identity, billing address, and more.
* **Unregistered SIMs:** Unregistered SIMs are pay-as-you-go SIMs that do not require identification for purchase. In some countries, registration is not required. In others, unregistered SIMs are sold on the black market. Recognize that SIMs given to you by another person (colleague, family member, acquaintance, or stranger) may *still* be registered, just not to you. They could, depending on the degree of separation between you and the person giving you the SIM, be tied back to you via human networks.

1b. **Discussion: Story of your SIM(s):** Ask participants how they obtained their SIMs (current and past), and the trade-offs of registered versus unregistered SIMs where they live and work.

Questions for Discussion:

* Are participants on prepaid plans or on contract? Do some have more than one SIM, of either or both types?
* Are participants using registered or unregistered SIMs?
* If unregistered, how did they get them?
* If registered, what kind of identification did they have to provide?
* Do they know of anyone who has gotten in trouble or had their service cut off for having/obtaining unregistered SIMs? Can they share advice as to where to buy them locally?
* What are the unique trade-offs to having registered versus unregistered SIMs in your community (price, privacy, legality, etc.)? Is it possible to use an unregistered SIM?

**2. Instruction (15 - 30 minutes):** Intro to identity on mobile networks.

2a. **MNO subscriber records** (*who they think you are*)

This is however you are registered (registered or unregistered SIM), which they have in addition to records of usage on the network (below).

2b. **Unique identifiers** (*what you look like to an MNO*)

When a mobile device is on and in range of a GSM network, it is constantly communicating and logging the following **uniquely identifying information** via the network infrastructure:

* **The IMEI number:** the **international mobile equipment identity** number, which uniquely identifies the hardware of your mobile device (this is usually a handset, but can also include other mobile devices, such as a wireless modem).
* **The IMSI number:** the **international mobile subscriber identity** number, which uniquely identifies the SIM card. This is tied to a user’s account and phone number.
* **The TMSI number**: the **temporary mobile subscriber identity** number, a temporary number that is re-assigned regularly according to location or coverage to help manage roaming and other services.

2c. **Geolocation** (*where you are*)

The mobile device is also performing geolocation(tracking where you are) on network, location, and content and usage:

* The network cell in which the phone is located. Cells can cover any area from a few meters to several kilometers, with much smaller cells in urban areas and even small cells in buildings that use a repeater aerial to improve signal in the immediate area.
* The location of the subscriber within that cell. This is determined by triangulating the signal from nearby towers. Again, location accuracy depends on the size of the cell - the more towers in the area, the more accurate the positioning.
* Content and usage. It is important to realize that your mobile usage, including all your calls (both who you call and who you receive calls from), SMS, MMS, data usage, time and location of mobile access and usage, and more, are all pieces of data that can identify you individually or in aggregate. Remember that nearly all of this information can be seen and/or logged by the MNO. Even encrypted data usage, which cannot be “seen” at the MNO level, is tagged with the time and location where you accessed it, even if the content is not known.

2d. **Data logging by MNOs** *(what they collect and store)*

* MNOs keep a record of or log the uniquely identifiable information that is constantly communicated to and from the network (as described above), along with the use of mobile services subscribers use.
* The logging of the type, length, and times of service usage such as calling, texting, or web browsing is tagged with your uniquely identifying information and your location at the time. This is all tied to the record the MNO has associated with your registration, which is the information you provided when accessing services (such as buying a SIM or a handset).
* Typical logs will include:
  + All voice calls, including length of call, the initiator of the call, and the identifying information of all parties who participated in the call, and their approximate geolocations. Voice is usually encrypted once it enters the network, unlike SMS. MNOs have the ability to listen to voice calls, but usually only use this access upon the request of law enforcement or on the demand of governments in closed societies that depend heavily on surveillance.
  + The content of any SMS or MMS received or sent, and the identifying information of parties who sent or received the message. SMS are sent in plaintext (meaning they are not encrypted) as they pass through the network.
  + Any data services used, when that data was accessed, how much data was uploaded and downloaded, and the user’s identifying information. The content (such as which sites were visited or the content of emails) may or may not be stored, and users can prevent this by anonymizing their browsing (by using Tor, for example) and encrypting all communications. It is also important to note that some services or programs that are otherwise deemed secure and encrypted online may not be when used via mobile networks, especially some free and commonly used IM and VOIP clients.
  + Your approximate location on an ongoing basis, whenever your phone is on.

**3. Instruction (15-30 minutes):** Issues of identity.

3a. **How to obscure your identity on mobile networks**

* Because of the breadth and depth of information about mobile users that can be logged, mobile phones cannot be used in a truly anonymous manner. It is possible, however, to obscure your identity so that the effort required to link you to your mobile use is greater. For some activists, journalists, and rights defenders, this can be crucial.
* Obscuring your identity means you are using mobile services, but making it harder to associate unique identifying information about you with that usage.
* You must be able to access non-registered SIM cards in order to prevent associating your name and identity with your mobile device usage. However, if SIM registration is legally required or if your phone will not work with an unregistered SIM, this is a more difficult situation. You can make some of the following suggestions if applicable to a particular situation:
  + Buy your SIM somewhere *away* from where you are known and seen. Travel to another town or part of the city where you are not known.
  + If concerned about having your unregistered SIM confiscated or cut off, try to buy multiple unregistered SIMs to have on hand in case of emergency and if unregistered SIMs are hard to find and replace.
  + Remember that SIMs that are not used may become inactive, for example, after 6 months without any revenue-generating activity. How long does it take for SIMs to become inactive in your region, and how could this be avoided?
* Since handsets and all mobile devices are also uniquely identifiable by their IMEI numbers, it is suggested that users seeking anonymity obtain a handset in a manner that prevents it from being associated with them. Pay cash and buy second hand.
* Remember that MNOs (and those who can gain access to their records and logs) can see your SMS, MMS, unencrypted data usage, and listen to your calls. To stay anonymous, even if you believe you are not being actively monitored at the MNO level, do not send or receive any information that could identify you. You may also want to leave your phone off with the battery out in order to prevent having your physical location being tracked via the network.
* If you use data services, use encryption. Be very careful when accessing any online account that requires you to log in. If you are concerned about being identified, you should only do this while using an anonymizing tool like Tor (covered later).
* Keep in mind that if someone you are in contact with via your mobile is being watched or monitored, they could reveal your identity either accidentally or when placed under threat. This is relevant if you are operating in an high-risk context and the likelihood of surveillance is high.

3b. **How the identity of an ‘anonymous’ user might be discovered**

* The most common way to “reverse engineer” the identity of a user attempting anonymous mobile usage is via human networks. If someone in your network has their phone taken or confiscated and your real name and phone number is in the mobile address book, your anonymity is compromised. Those that have access to your phone can take that information to the MNO to collect more information on you or conduct monitoring of varying degrees. Entire networks or organizations attempting anonymity can be compromised in this manner, and if you are operating in a high-risk context, your only option may be to dump your SIMs and handsets. **Critical**: ***Remember that changing SIM cards is not enough: handsets can still be tracked via their unique IMEI numbers.***
* Other human network considerations: A member of your network could be sloppy with your identity and phone number in other ways, such as communicating it insecurely or allowing it to be physically overheard.
* If someone is trying to identify you via phone usage and has access to MNO data and records, realize that they can read any SMS you send or receive in plaintext and any identifiable information contained within. Depending on the level of access at the MNO level and the monitoring capabilities available, a person can listen into your voice calls and view any unencrypted data services that you access as well.
* Keep in mind that if you are getting an unregistered SIM from a friend, family member, or colleague who can be associated with you, a little bit of investigation by those with access to MNO records may be able to reverse engineer the likelihood that you use that contact’s old SIM.

3c. **Unlocked/jailbroken/rooted devices**

Trade-offs when using locked/unlocked devices:

* Some individuals will use unlocked devices in order to use them on networks other than the network they were with then they purchased the phone. You may also use or have heard of people using ‘jailbreaking’ and ‘rooting’ devices in order to use certain unauthorized applications on them (in particular, jailbreaking for iPhones and rooting for Android phones). In fact, some security apps require a rooted phone. Some people believe that the modified operating systems that can be installed on rooted Android phones (e.g. CyanogenMod) may be more secure than the phone’s stock operating system.
* Although these can be useful, they can also have security implications. Rooted, jailbroken, or unlocked devices can disable certain features on some phones, including automatic updates that address vulnerabilities identified by the company behind your devices particular OS.
* In general, unlocking should only be done with good reason. Rooting and jailbreaking should only be done if you are technically proficient enough to understand and address the security implications.

**4. Things to highlight**

* Your phone and your SIM are uniquely identified. If there is a way to identify you as their owner, your identity can be is linked to your phone use.
* The location of your phone can be triangulated (through the MNO, through your human network, or through content you share).
* Mobile networks keep extensive records of your communications, including both content and time/location.
* Be deliberate with how you allow your devices to track your whereabouts and share your information.
* During and while travelling to sensitive meetings, take batteries out of phones.
* Do your best to keep your hardware (both handset and SIM) unattached to your identity.
* Avoid sharing information that can be used to identify you.
* Some information may be too sensitive to share over mobile networks at all.