### Example: Risk Assessment Worksheet for MobileActive.org

We’re an NGO that operates out of New York City, travels to various countries with different operational environment. Many of us are politically active and participate in protest action; at times we also act as citizen journalists. We use both smartphones (iPhones, Android, Blackberry) and feature phones (Nokia S40 and S60). We store a lot of information on our phones and we use them for both work and personal communication.

*Given this scenario and the variation in operational environments between US and abroad, we have chosen to divide our policy and assessment into 2- US and abroad. The assessment reflects this.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Use Case** | **Modalities Used** | **Risk** | **Impact (risk level - public, low, medium, high)** | **Likelihood (low, medium, high, expected)** | **Mitigation ideas** |
| call each other about schedules and meeting places | voice | someone will know who, when, and where you are meeting; the phone numbers of your contacts may be identified; your location at time of call may be known | US - low; abroad - potentially high depending on parties | expected | use skype, use redphone, look around when making phone calls in public places to see if we are being overheard |
| email about work, scheduling, planning, travel, personal | email, mobile data, email service provider | emails stored on the phone may be read by someone who gets hold of the phone. emails stored on the server may be read if the server is compromised, email may be intercepted if sent over insecure connections. someone may impersonate us over email. | US and abroad - high; we consider the content of our work and personal emails private between ourselves and the other parties | low to medium | always use SSL when downloading mail to a mail client or mail app, always use https when accessing our webmail. consider using encrypted email for particular contacts or particular sensitive information |
| Tweet, post Facebook status updates | mobile web, online services (Facebook, Twitter) | your location may be known; your login details may be intercepted and someone may be able to access your account unauthorized; someone may be able to impersonate you | location: US - low; abroad - low/medium  login details: US and abroad - high | location: low  login details: high | use https for all login details, and only use facebook and twitter apps and mobile sites that we know handle our login details safely. use strong passwords. use the available security settings for online accounts |
| we take photos and post on flickr, Facebook, Twitter. The photos are usually meant to be public | media, mobile web/data, online services (Facebook, Twitter), mobile app | photos stored on the phone can be viewed/copied by someone who gains access to the phone. | US and abroad - low; we intend to post most photos and so aren’t too concerned about where they might end up | low | no change - intended to be publi |
| live stream to Bambuser | media, mobile data, online services (Bambuser) | you are identified as a participant at an event; people you film could be identified as participants in a certain event | US and abroad -- medium; if being identified as participating in an event could be dangerous, high |  | only stream with consent from subjects, in ‘safe’ situations where their being identified would not put them in danger |
| skype contacts in US and other countries | mobile data, online services (Skype), voice services (US and other countries) | your call could be eavesdropped | US - low, abroad, medium to high depending on contact’s operational environment | US - low, abroad, depends on operational environment but usually low |  |
| store lots of contact info on phone -- everything from google/gmail account | phone storage, online services (Gmail) | contact information is accessible if phone is lost or stolen | US - low, abroad - possible high risk to contacts if they want to be anonymous | medium | use InTheClear so that phones can be wiped remotely |
| maintain calendar of events -- work meetings, work tasks, personal plans, incl Google Calender | phone storage, mobile data/mobile web, online service (Google Calendar), calendar app | events/plans are accessible if phone is lost or stolen, or if server is compromised, or if the app sends data using an insecure connection. | US: low, abroad, depends on sensitivity | lost/theft: medium, server compromise low, eavesdropping: low in US, possibly higher abroad. | don’t store sensitive information in calendar; use InTheClear to wipe phone if lost or stolen |
| send SMS to work and personal contacts | SMS | SMS can be intercepted or filtered, is logged by MNOs and can be accessed on a lost or stolen phone | US: low. abroad could be higher, depends on operation environment, sensitivity | interception/filtering: low in the US, possibly higher elsewhere. logging expected, lost/stolen phone medium | don’t send sensitive information via sms |
| receive email and store on phone | mobile data, email app, email provider | email can be intercepted, email stored on phone is vulnerable if phone is lost or stolen, email on server is vulnerable if server is compromised, email apps may communicate insecurely | medium - very sensitive information is not usually sent by email | US: medium for phone loss/theft, low otherwise, other countries may be different | use InTheClear so that phones can be wiped remotely |
| use maps and GPS to get around | location, mobile data/mobile web | MNO and map provider know my location | low, location is not usually sensitive/we don’t expect to be followed | expected |  |
| browse the Internet with whatever the default browser is | mobile web, browser app, phone storage (web history) | online account details (saved passwords) and history are vulnerable if phone is lost or stolen | web history - low. online accounts - high. | medium | don’t save passwords on phone browsers, use InTheClear so that phones can be wiped remotely |
| use Google Voice numbers to receive some, not all work calls | online services (Google Voice), mobile web (voice over IP) | Google and your MNO can log your calls, calls could be eavesdropped | low, except for calls with contacts who may not wish to be identified - medium | logging - routine, eavesdropping - low | offer contacts who do not wish to be identified alternate ways to contact us |
| use gChat | mobile web/wifi, online services (Google Talk), app | Google can and eavesdrop log chats, others on insecure wifi networks could intercept if app was not communicating securely | low; sensitive information is usually not shared on gchat | logging: routine, interception: low in US, may be higher elsewhere | don’t allow gChat to log conversations, don’t use gChat for sensitive information |
| use wifi | mobile web, mobile data | my traffic might be intercepted and my account details stolen if I am browsing non-https sites  when travelling, sites are sometimes blocked | theft of account details if not browsing securely  unable to access some sites/services | theft of account details: medium to high if not browsing securely  unable to access services: low in US, may be high elsewhere | only use encrypted (WPA2 ideally) wifi networks! always use https when doing anything where data or login details might be eavesdropped |
| create wifi network for my computer | mobile web, mobile data, apps | others might try to connect to my wifi network, and intercept my traffic | high | medium - mostly phone hotspot apps create open wifi networks or WEP-encrypted networks. WEP is easy to crack. | use a USB cable to tether instead. |
| use Google Latitude | location, mobile data, app | Google knows where you are and where you’ve been. | low | expected |  |
| keeps notes -- work and personal | app, phone storage | notes may be viewed by someone who gains access to the phone | low - most notes aren’t sensitive | medium |  |