Centre for Law & Transformative Change
Humanising Law & Justice

BABSEACLE

SECURE AND ENCRYPTED
LEGAL PRACTICE
IN HIGH SURVEILLANCE CONTEXTS

A DIY PRACTICAL GUIDE FOR DEFENCE LAWYERS

Protecting client confidentiality, securing communications, and maintaining basic digital hygiene in environments where legal practice is monitored, restricted, or at risk.

This guide does not require technical expertise. Every step described here can be taken by any lawyer with a smartphone and a willingness to build better habits. It is designed for contexts where courts, communications, and lawyers themselves may be subject to surveillance, pressure, or interference.

HOW TO USE THIS GUIDE

Priority Flags

- DO NOW - baseline protection: do this regardless of any specific threat
- DO BEFORE COURT - specific preparation before any hearing
- GOOD PRACTICE - additional steps when threat level is elevated

What This Guide Covers

- A. Know Your Threat Landscape
- B. Secure Your Devices
- C. Communicate Safely with Clients
- D. Protect Client Files
- E. In the Courtroom and Outside
- F. If You Are Targeted
- G. Recommended Tools at a Glance
- H. Personal Security Audit

A note on language

- This guide uses plain language throughout. Technical terms are explained when introduced. You do not need an IT background to follow any step described here.
- The guide reflects the reality that no security measure is absolute. The goal is to raise the cost and difficulty of surveillance and interference and not to promise invulnerability.

A Know Your Threat Landscape

Before choosing tools, understand what you are protecting against

The first rule of security is specificity. Not every lawyer faces the same risks. A lawyer representing a petty theft defendant faces different threats than one representing a political prisoner, journalist, or activist. Knowing your threat landscape allows you to focus your effort where it matters.

Common threats in high-surveillance legal environments

Threat	What it means for your practice	Your first response
Phone interception	Calls and unencrypted messages between you and your client are monitored in real time or recorded.	Move all sensitive communication to encrypted apps. Treat every standard phone call as if it is being recorded.
Device seizure	Your phone, laptop or office computer is seized by police, security services, or at a checkpoint.	Store as little sensitive material on the device as possible. Encrypt everything that is stored. Use app passwords in addition to screen lock.
Office search or raid	Your office is searched, files seized, or your staff are questioned.	Minimise paper files containing sensitive case information. Store digitally with encryption. Know your rights on search warrants and challenge unlawful searches.
Informants and infiltration	A client, witness, colleague, or third party is reporting on your work to state authorities.	Compartmentalise case information. Apply need-to-know principles. Be cautious about what you discuss in shared spaces.
Physical surveillance	You are followed, photographed, or your movements are monitored.	Vary your routine. Note unusual patterns. Report to your bar association and trusted colleagues. Document systematically.
Digital account access	Your email, cloud storage, or social media account is accessed without your knowledge — by hacking or by compelled access.	Use two-factor authentication on every account. Use strong unique passwords. Review account activity regularly.
Malware and spyware	Malicious software is installed on your device — sometimes through a single click on a link or an attachment.	Never click unexpected links or attachments. Use a separate device for sensitive work if possible. Update software regularly.

✓ Ask yourself three questions before you start any sensitive case

- Who specifically might want access to my communications, files, or client information in this case?
- What is the likely method they would use? (Phone interception? Device seizure? Informant? Cyber access?)
- What would be the consequence for my client if they succeeded?

Your answers determine your threat level. Higher threat = higher precautions. Not all cases require the same level of protection.

B Secure Your Devices

Your phone and laptop are the most vulnerable point in your practice

Most surveillance of lawyers begins with their device. An unsecured phone is an open window into your practice. These steps apply regardless of the level of your current threat.

PRIORITY	ACTION	WHY IT MATTERS
DO NOW	Set a strong screen lock. Use a minimum 6-digit PIN or alphanumeric password. Fingerprint or face ID alone is not sufficient in environments where you may be compelled to unlock your device physically.	*A PIN cannot be compelled with your finger or face pressed against the sensor. In many jurisdictions, compelling a PIN is legally and practically harder than biometric access.*
DO NOW	Enable full-device encryption. On Android: Settings > Security > Encryption. On iPhone: enabled automatically with a passcode set.	*If your device is seized, an encrypted device is far harder to extract data from without the passcode.*
DO NOW	Set auto-lock to 30 seconds or less. A device left on a desk for two minutes unattended is a device that can be accessed.	*Most physical access incidents occur during short windows of inattention.*
DO NOW	Enable remote wipe. On Android: Google Find My Device. On iPhone: iCloud Find My. Register the device and test that you can wipe it remotely.	*If your device is seized or lost, you can erase all data before it is forensically examined.*
DO NOW	Turn off Bluetooth and Wi-Fi when not in use, particularly in or near courts, police stations, and government buildings.	*Bluetooth and Wi-Fi broadcast your device identity and can be used to track your location or initiate a connection you have not authorised.*
DO BEFORE COURT	Before attending court, a police station, or a government office: delete any draft messages, remove any sensitive files from the device to encrypted cloud storage, and restart the device (this clears RAM and re-requires the passcode for some access methods).	*Some forensic and legal access methods are defeated or significantly complicated by a device that has been restarted and not yet unlocked.*
DO BEFORE COURT	Consider carrying a second, minimal device to sensitive locations — a cheap phone that holds only what is needed for that day, and nothing else.	*A seized minimal device reveals minimal information.*
GOOD PRACTICE	Keep your operating system and all apps updated. Updates contain security patches that close known vulnerabilities.	*Most successful device hacking exploits vulnerabilities in outdated software.*
GOOD PRACTICE	Install only apps from official app stores. Delete apps you do not use. Each installed	*Unused apps continue to request permissions and run in the background.*

GOOD PRACTICE	app is a potential access point. For your most sensitive work, consider a separate device that you use only for that purpose, never for social media, entertainment, or other browsing.	*Separating your sensitive work device from your everyday device substantially reduces your attack surface.*

C Communicate Safely with Clients

The channel you choose determines the security of what you say

Standard phone calls and SMS text messages are interceptable without technical difficulty in most high-surveillance environments. Assume they are monitored. Use encrypted messaging apps for all sensitive communications with clients and colleagues.

The hierarchy of communications security

Level	Method	Use for
Most secure	In person, in a private space, with phones left in another room or switched off	*The most sensitive case discussions. Plea decisions. Client instructions on high-risk matters.*
↓	Signal (encrypted messaging + calls, disappearing messages enabled)	*Daily client communication. Sending documents. Voice calls when in person is not possible.*
↓	ProtonMail or Tutanota (encrypted email between users of the same service)	*Formal correspondence. Sharing documents that require a record.*
↓	WhatsApp (end-to-end encrypted but linked to your phone number and metadata visible to Meta)	*General communication where Signal is not possible. Not for highest-risk cases.*
↓	Standard email (Gmail, Yahoo, unencrypted services)	*Non-sensitive administrative matters only. Assume it can be read by third parties.*
Least secure	Standard phone call or SMS	*Assume all calls and texts are monitored. Never discuss case strategy, client identity, or sensitive facts on these channels.*

Setting up Signal: the five essential steps

PRIORITY	ACTION	WHY IT MATTERS
DO NOW	Download Signal from the official app store (Signal.org/install). Do not download from unofficial sources.	*Signal is free, open-source, and independently audited. It is the industry standard for encrypted messaging.*
DO NOW	In Signal Settings: enable Registration Lock. This prevents your Signal account being transferred to another device without a PIN you set.	*Protects your Signal identity if your phone number is compromised or transferred.*
DO NOW	In Signal Settings > Privacy: enable a Screen Lock for Signal itself, separate	*Means that even if your device is unlocked, Signal requires a second entry to open.*

	from your device lock.	
DO NOW	For sensitive conversations: set Disappearing Messages. 1 week is a reasonable default for most client communications. Use 24 hours for the highest-risk exchanges.	*Messages that no longer exist cannot be compelled or seized. Disappearing messages also protect clients who may have their own devices accessed.*
DO NOW	Advise your client to use Signal also. Walk them through the setup if needed. A secure channel is only secure at both ends.	*An encrypted message to an unencrypted device provides no protection at the receiving end.*
GOOD PRACTICE	Use Signal's Note to Self feature as a private encrypted scratchpad for case notes you need on your phone.	*An alternative to noting sensitive case information in an unencrypted notes app.*

⚠ Metadata: what encryption does not protect

- Encrypted messaging protects the content of your messages. It does not conceal the fact that you communicated, with whom, at what time, and for how long.
- In high-surveillance environments, metadata can be as revealing as content. Authorities may infer a great deal from the pattern of your communications with a client, even without reading the messages.
- For the most sensitive cases: vary the timing and frequency of communications. Conduct the most critical conversations in person.

D Protect Client Files

Digital files require the same confidentiality obligations as paper

Client files in an unencrypted folder on your desktop are as vulnerable as paper files left on an open desk. The following steps apply to how you store, name, share, and dispose of client documents.

PRIORITY	ACTION	WHY IT MATTERS
DO NOW	Use a cloud storage service with strong security for all client files. Google Drive (with full-device MFA enabled) is adequate for most cases. For high-risk cases, use Proton Drive or a Cryptomator-encrypted vault inside any cloud service.	*Do not store sensitive files locally only. A seized device containing unencrypted local files is fully readable. Cloud storage with encryption separates the file from the device.*
DO NOW	Enable two-factor authentication (2FA) on every account that holds client data: Google, Dropbox, OneDrive, email. Use an authenticator app (Google Authenticator, Authy) — not SMS alone.	*SMS-based 2FA can be defeated by SIM-swap attacks. An authenticator app generates codes on your device independently of your phone number.*
DO NOW	Use a password manager (Bitwarden is free and open-source) to generate and store strong unique passwords for every account. Never reuse a password.	*A password reused across accounts means that one breached account gives access to all.*
DO NOW	Do not store client names or identifying details in file names or folder names that are visible in cloud storage. Use matter numbers or codes instead. Keep the key (number to name) in a separate encrypted location.	*File names and folder structures are often visible even in previews, shared links, and metadata, before the file is opened.*
DO BEFORE COURT	Before any hearing: confirm that court documents, witness statements, and case strategy notes are not in unencrypted folders on devices you will carry to court. Move them to cloud storage and delete the local copy.	*Anything on a device you carry to court is at risk of seizure at the door.*
DO BEFORE COURT	Apply strict sharing controls. Share documents only with named individuals using restricted links. Never use an open link that anyone with the URL can access.	*An open sharing link sent to a client is accessible to anyone who obtains that link — by forwarding, by accessing the client's device, or by interception.*
GOOD PRACTICE	For the most sensitive files: use Cryptomator. This free tool encrypts a vault on your device before syncing to any cloud. The cloud provider and any authority accessing the cloud account sees only unreadable encrypted data.	*Zero-knowledge encryption means that even a court order directed at your cloud provider cannot produce readable files.*
GOOD PRACTICE	Establish a clear retention and deletion policy. Files that no longer exist cannot be	*Routine deletion reduces your exposure. The largest risk comes from files that were once*

	seized. Delete files you no longer need, and do so securely (use a secure deletion tool; deleted files remain recoverable from a hard drive until overwritten).	*sensitive and have since been forgotten.*

A note on email and confidential documents

- Standard email is not secure. Do not send sensitive documents — witness statements, instructions, case strategy, client identity information — by standard email.
- If you must send a sensitive document by email: password-protect the document using your PDF application, and send the password by a separate channel (Signal, or verbally).
- Between two Proton Mail or two Tutanota users: email is automatically end-to-end encrypted. For cross-service encrypted email, use ProtonMail's encrypted outbound feature or send a password-protected file.

E In the Courtroom and in the Field

The hearing room and the street present specific physical security risks

PRIORITY	ACTION	WHY IT MATTERS
DO NOW	Assume that conversations in courthouse corridors, consultation rooms, and holding cells may be monitored. Treat any room you did not independently verify as potentially surveilled.	*Surveillance equipment is compact and easily concealed. Consultation rooms provided by authorities should be treated with particular caution.*
DO NOW	When consulting with a client in a detention facility, be aware of whether staff are within earshot. Request a private consultation room. If refused, note and document the refusal as a fair trial issue.	*Under CRPD Art 13 and ICCPR Art 14, access to a lawyer in private is a fundamental procedural right. Denial can be challenged.*
DO NOW	Do not discuss strategy, plea considerations, or client identity with colleagues in public places: restaurants, shared transport, or open office spaces.	*Professional confidentiality extends beyond the office. Public spaces are the most common location for inadvertent disclosure.*
DO BEFORE COURT	Before attending a location you consider at risk: note in a message to a trusted colleague where you are going, who you are meeting, and when you expect to return. Agree a check-in time.	*A simple check-in protocol means that if you are detained, searched, or prevented from leaving, there is a record and a person expecting to hear from you.*
DO BEFORE COURT	Know who to call immediately if your device is seized, your office is searched, or you are questioned about your case. Have the number of your bar association and a trusted colleague saved and memorised.	*In a moment of sudden pressure, you will not have time to search for contact details.*
GOOD PRACTICE	When travelling to high-risk locations: leave unnecessary devices at a secure location. Carry only what you need. If crossing borders: log out of all sensitive apps, and use a travel profile with minimal data if possible.	*Border crossings, checkpoints, and security sweeps create opportunities for device access that are difficult to challenge in real time.*
GOOD PRACTICE	Photograph or scan case documents before court attendance. Store in encrypted cloud. If physical files are seized at court, you retain the digital copies.	*Physical seizure of paper files can be a tactic to disrupt your preparation. A backup means it cannot succeed.*

F If You Are Targeted

A prepared response prevents panic and preserves your rights

If you are subjected to surveillance, interference, or direct action, your response in the first hours is critical. Calm, systematic action protects both you and your clients.

Response Flow: Device Seizure

1	Do not resist the seizure physically. Your safety is the priority.	*State clearly and calmly: "I am a lawyer. These devices contain legally privileged material. I require that my bar association is notified before any examination."*
2	Note the time, location, officer identity, and agency.	*Ask for written confirmation of the seizure. If refused, note the refusal.*
3	As soon as you have access to any other device, notify: your bar association, a trusted colleague, and where appropriate, an international legal protection organisation.	*Frontline Defenders and the International Bar Association's Human Rights Institute (IBAHRI) both provide support to lawyers facing interference.*
4	Remotely wipe the seized device if you have enabled this.	*Balance this against the need to preserve evidence of the seizure itself if you intend to challenge it. Seek advice quickly.*
5	Document everything immediately: what was taken, what was on it, who took it, what they said.	*This documentation supports a legal challenge, a bar association complaint, and any international reporting.*

Response Flow: Account Compromise

If you believe your email, cloud account, or messaging account has been accessed without authorisation:

1. STOP using the compromised account for any sensitive communication immediately.
2. From a different, secure device: change the password and revoke all active sessions (in most accounts: Settings > Security > Active Sessions > Sign out all).
3. Revoke access from all third-party apps connected to the account.
4. Check the account's activity log for sign-in locations and times you do not recognise.
5. Inform clients who may have sent sensitive information to that account that it may have been compromised.
6. Generate new backup codes and review all 2FA settings.
7. Consider whether the compromise was targeted (high-risk: change all related accounts) or opportunistic (lower-risk but still review all passwords).

Know these contacts before you need them

- Bar association emergency contact: _____
- Frontline Defenders (protection of human rights defenders): www.frontlinedefenders.org | +353 1 210 0489
- IBAHRI (International Bar Association Human Rights Institute): www.ibanet.org/IBAHRI
- Digital Frontline Fund / Access Now Digital Security Helpline: accessnow.org/help
- Trusted colleague contact (memorise this): _____

Fill in the first and last lines now. Do not leave them blank.

G Recommended tools at a Glance

Practical, low-cost, and accessible tools for defence lawyers

All tools listed below are free or have a free tier sufficient for individual lawyer use, unless noted. All are available on Android and iOS unless stated.

Communications

Tool	Where	Use it for	Cost	Difficulty
Signal	iOS / Android	Encrypted messaging, voice and video calls, disappearing messages. The gold standard for sensitive legal communication.	Free	Easy
ProtonMail	Web / iOS / Android	Encrypted email. End-to-end encrypted between Proton users. Use for formal correspondence when email is required.	Free tier	Easy
Tutanota	Web / iOS / Android	Encrypted email alternative to ProtonMail. Similar feature set.	Free tier	Easy
ProtonVPN	Web / iOS / Android	VPN from Switzerland. No-log policy. Use on all public Wi-Fi. Free tier available.	Free tier	Easy

Files and Storage

Tool	Where	Use it for	Cost	Difficulty
Proton Drive	Web / iOS / Android	End-to-end encrypted cloud storage. Files cannot be read by Proton or governments. Best for highest-risk files.	Free tier	Easy
Cryptomator	Desktop / iOS / Android	Creates an encrypted vault inside any cloud service (Google Drive, Dropbox, etc.). You hold the key. Free on desktop.	Free (desktop)	Medium
Bitwarden	Web / iOS / Android / browser	Open-source password manager. Generates and stores strong unique passwords. Sync across devices.	Free	Easy
Google Drive + 2FA	Web / iOS / Android	Adequate for most cases when full 2FA is enabled and sharing settings are correctly set to Restricted.	Free	Easy

Device Security

Tool	Where	Use it for	Cost	Difficulty
Google Authenticator / Authy	iOS / Android	Generates 2FA codes independently of your phone network. Use instead of SMS-based 2FA.	Free	Easy
Google Find My Device	Android / Web	Remotely locate and wipe an Android device. Set up before you need it.	Free	Easy
Standard Notes	Web / iOS / Android / Desktop	Encrypted notes app. End-to-end encrypted. Use instead of standard phone Notes for sensitive case notes.	Free	Easy

Tella	Android / iOS	Designed for human rights documentation. Encrypts photos, videos, documents on the device. Panic button to delete all.	Free	Easy

⚠ Tools to avoid for sensitive legal work

- Standard SMS / iMessage (unencrypted, carrier-accessible, or linked to Apple ID).
- WeChat, Telegram (standard chats) — chats are not end-to-end encrypted by default; user data subject to state requests in multiple jurisdictions.
- Dropbox and iCloud without additional encryption — US-jurisdiction providers, no zero-knowledge protection.
- Free VPNs from unknown providers — many log and sell your traffic data.
- Any messaging or email app that you have been sent by a client or unknown contact (could be malware).

H Personal Security Audit

Complete this checklist. Every unticked item is an open door.

This audit takes approximately 20 minutes. Complete it now. Return to it every three months and after any significant security incident or new high-risk case.

MY DEVICES	
☐	My phone has a strong PIN (6 digits or more) or alphanumeric password
☐	Full-device encryption is enabled on all my work devices
☐	Auto-lock is set to 30 seconds or less
☐	Remote wipe is enabled and I know how to use it
☐	I turn off Bluetooth and Wi-Fi in high-risk locations
☐	My operating system and apps are up to date
MY ACCOUNTS	
☐	Two-factor authentication (2FA) is enabled on ALL accounts holding client data
☐	I use an authenticator app, not SMS alone, for 2FA
☐	I use a password manager and unique passwords for every account
☐	I have reviewed recent login activity on my key accounts in the last month
☐	I know how to remotely revoke access to all active sessions on my accounts
MY COMMUNICATIONS	
☐	I use Signal for sensitive communications with clients and colleagues
☐	Disappearing messages are set on Signal for sensitive conversations
☐	I do not discuss case strategy on standard calls or SMS
☐	I have advised my clients on how to communicate with me securely
☐	I do not discuss sensitive matters in courthouse corridors, consultation rooms provided by authorities, or public places
MY FILES	
☐	Client files are stored with encryption (Proton Drive, Cryptomator, or cloud with 2FA minimum)
☐	Client file names and folder names do not contain client names or identifying details
☐	Sensitive files are not stored locally on devices I carry to high-risk locations

☐	I use restricted sharing only — no open sharing links on client documents
☐	I have a secure deletion practice for files I no longer need

MY PREPARATION

☐	I have identified the specific threat landscape for my current high-risk cases
☐	I have a check-in protocol with a trusted colleague for high-risk visits
☐	I know the emergency contacts for my bar association and at least one legal protection organisation
☐	I know the five steps if my device is seized (see Section F)
☐	I know the steps if my account is compromised (see Section F)

My security audit result

Date of audit: _____ Unticked items: _____

Three actions I will take this week:

1. _____
2. _____
3. _____

Next audit date: _____

LEGAL BASIS: THE RIGHT TO PRACTISE IN SECURITY

The right of defence lawyers to communicate confidentially with their clients is not simply a professional preference. It is a fundamental component of the right to a fair trial and is grounded in binding international law.

Instrument	Relevance to Lawyer Security
UN Basic Principles on the Role of Lawyers (1990) — Principle 8	Lawyers must be able to perform their professional functions without intimidation, hindrance, harassment, or improper interference. Governments must ensure lawyers can consult with clients in confidence.
ICCPR Article 14(3)(b)	The right to communicate with counsel of one's own choosing. Confidential communication is inherent in this right.
ICCPR Article 17	The right to privacy. Surveillance of lawyer-client communications requires legal basis, necessity, and proportionality.
UN Declaration on Human Rights Defenders (1998) — Articles 1, 12	Lawyers acting as human rights defenders are entitled to protection from surveillance, harassment, and interference with their work.
CRPD Article 13	Access to justice includes access to effective legal representation. Surveillance that deters or compromises legal representation breaches this right.
UN Special Rapporteur on the Independence of Judges and Lawyers	Multiple reports have documented the use of surveillance against defence lawyers as a structural attack on judicial independence and fair trial rights. Reports available at: ohchr.org/en/issues/judges-and-lawyers
Mendez Principles (2021)	Principles on Effective Interviewing for Investigations and Information Gathering. Affirm that legal consultation must be private and free from monitoring.

Using this legal basis in practice

- If your consultation room is monitored or access to private communication with your client is denied: cite UN Basic Principles Principle 8 and ICCPR 14(3)(b) in your immediate written objection.
- If your devices are seized without lawful authority: cite ICCPR Article 17 (right to privacy) and demand written grounds.
- If you are being harassed for representing an unpopular client: cite the UN Declaration on Human Rights Defenders and notify your bar association, IBAHRI, and the Special Rapporteur.
- Document every incident. Pattern evidence creates the strongest case for systemic challenge.

QUICK REFERENCE SUMMARY

DO THESE NOW (baseline, every case)

- Strong PIN + full-device encryption on all devices
- Two-factor authentication on all accounts
- Signal for all sensitive client communications
- Disappearing messages enabled on Signal
- Password manager with unique passwords
- Remote wipe enabled and tested
- Restricted sharing only on all client files

DO BEFORE COURT (every hearing)

- Move sensitive files off the device to encrypted cloud
- Delete local copies of sensitive documents
- Check-in protocol activated with a trusted colleague
- Emergency contacts ready and memorised
- Device restarted
- Know your rights on device seizure and have your objection language ready

IF DEVICE SEIZED

- → Do not resist physically
- → State: legally privileged material, bar association must be notified
- → Note officer identity, time, location
- → Notify bar + colleague immediately from another device
- → Remotely wipe if appropriate
- → Document everything

KEY CONTACTS

Bar association: _____
Trusted colleague: _____
Frontline Defenders: +353 1 210 0489
Access Now Helpline: accessnow.org/help
IBAHRI: ibanet.org/IBAHRI

Prepared for use by the Centre for Law & Transformative Change (CLTC) and BABSEACLE for defence lawyers in Asia and other high-surveillance legal environments.