# **Technology** Audit

### Identifying a client's devices, apps and online accounts

#### Key safety requirements

- Any technology safety planning is done in the context of broader family, domestic and sexual violence risk assessment and safety planning tools.
- Any changes to technology and device use are only made after considering a client's specific situation and safety.
- In some cases, it may be safest not to make any changes to a client's device or technology to avoid triggering further violence.

#### Using this auditing document

- This is not an exhaustive list. It includes examples of the more popular devices, apps and online accounts. We recommend asking clients to think about any other technology they use and is not listed.
- To help inform current and future safety planning, devices, apps and online accounts have been flagged when their settings and capabilities could be used by an abuser to track, coerce or harm a client. Specifically, the potential for:



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera



connecting to wi-fi, bluetooth or GPS (device-level only)

~~
T I
203

spyware infection (device-level only)

- These safety considerations should be used as a guide only.
- There is a column for the client to note whether the abuser had access to a particular device, app or online account, or is likely to have had access.
- If a client has any children in their care, we recommend doing a separate audit of their devices, apps and online accounts.
- We also recommend prompting clients to think about any work devices, apps or online accounts their abuser might have accessed.

### Need help to support your client?

Request a call back from eSafety's Technology-Facilitated Abuse Support Service via the **enquiry form**.

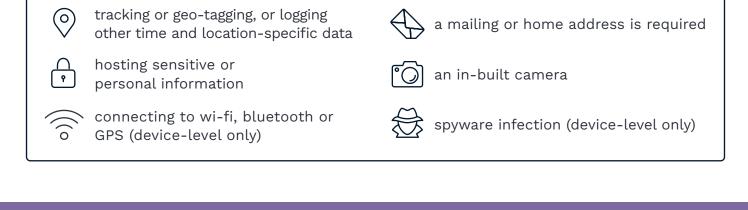
The TFA Support Service (the Service), and the information provided through it, are provided 'as is' (and as a guide only) and are not a substitute for professional advice (whether medical, clinical, legal, technical, or otherwise). You should not rely on the Service to make any decision, and you are encouraged to seek professional advice if appropriate. For more information about how the Service can be used, and its limitations, please read the full <u>Terms and Conditions</u>.





## **Client technology audit**

Category: personal devices		
ltem	Safety considerations	Tick if abuser ever had access
Laptops	000000000000000000000000000000000000000	
Mobile phones	$\bigcirc \bigcirc $	
Mobility aids and assistive technology	000000000000000000000000000000000000000	
Tablets: iPad, Galaxy Tablet	000000000000000000000000000000000000000	
Fitness watches	♥ ⊕  ⊕	
Smart watches	0 € € €	
Home modems	$\bigcirc \bigcirc $	
USBs and portable hard drives	f 😓	
Bluetooth headphones	(((0	
Other:		



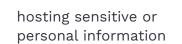
Category: location and travel			
Iten	1	Safety considerations	Tick if abuser ever had access
	Dashcams	000000000000000000000000000000000000000	
	GPS devices: Garmin, Navman	$\bigcirc \bigcirc $	
	Pet microchip	$\bigcirc \bigcirc $	
	Tracking devices: AirTags/SmartTags/Tiles	0       	
	eToll and/or Linkt account	◎ 🕂 🚸	
	Location-sharing apps: Life360, Findmykids, Pingo	$\bigcirc \ \varTheta \ \diamondsuit$	
	Ride-share and taxi accounts: Uber, DiDi, Ola	◎ 🕂 🕀	
	Transport cards and accounts: Opal, Myki	$\bigcirc \ \bigcirc \ \diamondsuit$	
	Bike/scooter sharing apps: Lime, Beam	00	
	'Find My Device' accounts	00	
	Map apps: Google Maps, Apple Maps	00	
	Parking accounts/apps	00	
Othe	er:		



 $\bigcap_{\mathbf{P}}$ 

(()

tracking or geo-tagging, or logging other time and location-specific data



connecting to wi-fi, bluetooth or GPS (device-level only)



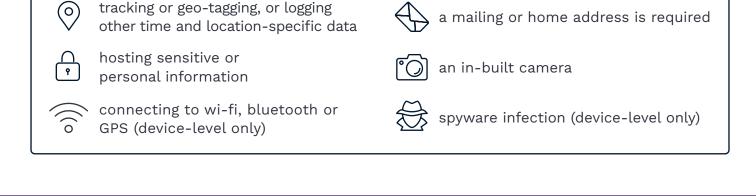


an in-built camera



spyware infection (device-level only)

#### **Category: sensitive and personal information** Tick if abuser ever Safety considerations Item had access Cloud storage: iCloud, Google Drive, 0 • Dropbox, One Drive Health accounts/apps: HotDoc, Health Connect, Samsung Health $\bigcap_{r}$ 0 Mobile phone accounts Government services accounts/apps: 0 MyGov, Medicare, Centrelink, ATO, digital driver's license Online calendars: 0 $\bigcap_{\mathbf{r}}$ Google, Outlook, iCal, Samsung $\bigcap_{\mathbf{r}}$ Email: Gmail, Outlook, hotmail Fitness accounts: A Apple Fitness+, Google Fit, MapMyRun Other:



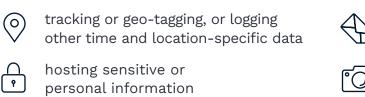
Category: children		
Item	Safety considerations	Tick if abuser ever had access
Drones	$\bigcirc \bigcirc $	
Baby monitors	$\begin{array}{c} \begin{array}{c} \begin{array}{c} \\ \end{array} \end{array} \end{array} \end{array} \\ \begin{array}{c} \end{array} \\ \begin{array}{c} \end{array} \end{array} \\ \begin{array}{c} \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} $	
Smart toys, including voice command	$\begin{array}{c} \begin{array}{c} \begin{array}{c} \\ \end{array} \end{array} \end{array} \end{array} \\ \begin{array}{c} \end{array} \\ \begin{array}{c} \end{array} \end{array} \\ \begin{array}{c} \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} $	
Other:		

Category: social media		
Item	Safety considerations	Tick if abuser ever had access
Facebook		
Foursquare	0	
Instagram	0	
Snapchat	0	
TikTok	0	
X (Twitter)	0	
YouTube	0	
Reddit	$\bigcirc$	
Other:		





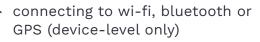
Category: home and lifestyle			
Iten	n	Safety considerations	Tick if abuser ever had access
	Alarm systems	$\bigcirc \bigcirc $	
	Security cameras	$\bigcirc \bigcirc $	
	Gaming, including consoles, accounts, apps	000000000000000000000000000000000000000	
	Virtual assistant: Google Nest, Amazon Alexa	000000000000000000000000000000000000000	
	Any smart electronics: TVs, washing machines, kettles, speakers, vacuum		
	Family Library		
	Family Sharing		
	Food delivery services: Uber eats, Door Dash, Menulog	$\bigcirc \diamondsuit$	
	Grocery/supermarket/chemist accounts with delivery services	$\Leftrightarrow$	
	MyPost account	$\Leftrightarrow$	
	Online shopping accounts/apps with delivery services: clothing, beauty, accessories	$\bigcirc$	
	Utilities (electricity, internet, water, gas)	$\Leftrightarrow$	
Oth	er:		



a mailing or home address is required



an in-built camera



spywa

spyware infection (device-level only)



()

Category: finance		
Item	Safety considerations	Tick if abuser ever had access
Afterpay	$\bigcirc \diamondsuit$	
Insurance accounts (health, car, home)	$\bigcirc \diamondsuit$	
Investment apps/accounts (CommSec, Stake, Selfwealth)	$\bigcirc \diamondsuit$	
Online bank accounts (credit/debit cards)	$\bigcirc \diamondsuit$	
PayPal	$\bigcirc \diamondsuit$	
Other:		

#### **Category: work and education** Tick if abuser **Safety considerations** Item ever had access Anydesk <del>م</del> LogMeIn $\bigcap_{r}$ My Uni Shared working or learning accounts: $\bigcap_{\mathbf{v}}$ Moodle, Blackboard $\bigcap_{r}$ Teamviewer Other:



