Australian Government
Department of Home Affairs

Scenarios – industry assistance to law enforcement and national security agencies

How are you affected by the industry assistance framework introduced by the Assistance and Access Act? Until you are approached to offer assistance, you are not required to make any changes to your business operations. If you are approached, your rights and obligations may depend on the size of your business and the nature of your business's relationship to communications technology.

These hypothetical case studies offer some examples of the industry assistance process in action. They are tailored to the many different situations that may be confronted by technology providers, investors and Government agencies.

More information on the Act can be found on the Department of Home Affairs website - www.homeaffairs.gov.au.

The information contained in this document is not legal advice.

Contents

RapID – A small-to-medium size enterprise

The industry assistance framework may affect entities in different ways. Agencies take this into account when formulating requests for assistance. The unique circumstances of small-to-medium size enterprises (SMEs) may mean that industry assistance may affect them differently compared to larger companies. As in the case of RapID below, operators of SMEs can seek information and assurances where they feel their ordinary business operations will be adversely affected by servicing a call for assistance.

Company background: RapID, a small-to-medium size enterprise employing thirty developers, runs a digital wallet for verified digital copies of identification documents. Users upload documents to RapID using end-to-end encryption through which the documents are verified and permanently erased from the servers. RapID is interested in having its identity verification technology used by traffic authorities and in airports.

Problem: A counterfeit document ring favoured by foreign fighters attempting to travel to conflict zones is known to be using RapID to test the quality of their fake passports. The foreign fighters are committing a serious offence (defined as an offence resulting in at least three years imprisonment), which in this case is the production and possession of false travel documents.

Action: A law enforcement agency contacts RapID to discuss obtaining assistance under a technical assistance request to collect copies of documents uploaded to the service from specified IP addresses. The matter is referred to RapID's CEO, Sadie, who explains that the company already has the expertise and existing capability to retain documents from particular IPs. However, Sadie would prefer the agency issue a compulsory notice (a technical assistance notice), rather than a voluntary request for assistance.

Discussion: Sadie raises concerns with the agency that providing the assistance requested will disrupt business operations and that she and her employees will receive financial (civil, not criminal) penalties if they fail to offer assistance. The agency invites Sadie to detail the potential impacts of the technical assistance notice on RapID to help the agency determine whether the requirements in the notice are reasonable and proportionate. The agency assures Sadie that RapID will not be penalised where it has reasonably tried to assist.

Result: RapID is issued a technical assistance notice requiring them to retain documents uploaded from a set of IPs known to belong to foreign fighters who are using RapID's product to commit the serious offence of travel document fraud. A RapID engineer makes the technical changes required by the TAN and the company is compensated for the reasonable cost of this work. The law enforcement agency then obtains and serves a search warrant on RapID to collect any documents retained in connection with the counterfeiters' IP addresses.

Business impact: RapID is committed to maintaining a reputation for transparency. Though they cannot disclose the purpose of the technical assistance notice, RapID can disclose the total number of notices they have been served with. RapID can further state it is their policy only to provide user data in response to warrants or authorisations.

Jogg Mobile – Building new capability

In certain situations, industry assistance will allow for the construction of new software or hardware capabilities around providers' systems in order to enhance their ability to assist in a law enforcement or intelligence activity. This is possible voluntarily through a technical assistance request or under an obligation connected with a technical capability notice. In most cases, these changes will not relate to security features.

Company background: Jogg is a discount mobile provider founded in 2015 that now employs 250 people. Jogg aims to provide low-cost mobile services by forgoing some of the features offered by premium networks and using older hardware.

Problem: Jogg's dated infrastructure means that the network does not have the capability to retain visitor location register (VLR) data – including location data of subscribers' devices when they are not communicating. This makes Jogg an attractive network for individuals looking to conceal their activities from law enforcement and intelligence agencies.

Action: An intelligence agency contacts Jogg through a public relations email address and is referred to Arthur – a member of Jogg's executive. The agency explains to Arthur it is monitoring users on Jogg's network suspected of belonging to a home-grown terror cell engaging in paramilitary training activities. The agency would like to upgrade Jogg's hardware to enable it to retain VLR data so that it can assist in the investigation of these users.

Result: Arthur, on behalf of Jogg, is generally willing to help – especially seeing the value of support to upgrade the network – but he remains cautious. Having not worked with government previously, Arthur considers a legal obligation to perform the upgrade offers the most certainty for the company. The Attorney-General gives Jogg a consultation notice to assess whether the proposed requirements meet the legal and technical tests. There is a 28 day consultation period. After this period, and with the agreement of the Minister for Communications, the Attorney-General issues a technical capability notice to Jogg requiring a system upgrade to enable Jogg to collect VLR data and negotiates a contract to cover the reasonable costs of the new equipment and hiring the required engineers.

Business impact: The upgrades to Jogg's network are noticed by tech bloggers and speculation suggests they are connected with government surveillance. Jogg issues a press release to clarify their policies for cooperating with government investigations. Jogg states that they only cooperate with government agencies when presented with a legal obligation and only hand over user data in connection with an appropriate warrant or authorisation.

Chipdex Inc. – A major American technology company

Companies that may be subject to assistance obligations include any provider of a digital service with at least one end-user in Australia. This includes large foreign companies that operate locally.

Company background: Chipdex is a major American legacy technology company with offices in 81 countries. Today, a significant part of the company's business is generated through cloud-based services such as data storage, email and web conferencing applications.

Problem: A leading Australian law enforcement agency learns that Chipdex's servers are being used to store child exploitation material. The agency serves a warrant on Chipdex and are supplied with the offending files. However, for compression purposes, the files are stored in a proprietary data format (.datr) that cannot be explored without specialist software. The warrant cannot compel Chipdex to re-encode the files and Chipdex have a policy of only supporting law enforcement following legal compulsion. Without a method of exploring the files, police must rely on bespoke solutions which add additional complexity and time to their work.

Action: Relying on previous consultation with Chipdex regarding .datr files, the agency issues Chipdex a technical assistance notice compelling the data to be provided in a readable format.

Result: Chipdex is required to provide the offending files in a readable format. Chipdex's reasonable costs of complying are repaid by the agency.

Business impact: Though Chipdex is an American company, they are connected to Australia through the location of their users, their regional office and some of their assets. Had Chipdex refused to comply with the technical assistance notice, enforcement action may have been taken in the Federal Court and the Chipdex body corporate may have been fined up to 10 million dollars.

Plain Old Telephone Service (POTS) – An agency perspective

The help available through industry assistance is subject to significant limitations. These limitations include the prohibition on building systemic weaknesses and creating vulnerability in a service or product, and the requirement that requests and notices must be reasonable, proportionate, and technically feasible. Because of these limitations, agencies may find situations where a designated communications provider cannot offer assistance. This is one such situation.

Company background: POTS is an over-the-top messaging and VoIP (Voice over Internet Protocol) platform that recently launched with the promise of securing user communications with an unbeatable new technology that guarantees exchanges are only visible to conversation participants. POTS insists it does not rely on end-to-end encryption but offers few other technical details.

Problem: Alongside interest from legitimate users, criminal elements quickly see the platform's potential to conceal their activities. This leads to an exodus from other communication platforms that frustrates many of the surveillance techniques relied upon by law enforcement and intelligence agencies.

Action: An agency has an active investigation into an organised crime group that uses POTS products. POTS has refused previous requests by the agency to examine the platform's technology under a technical assistance request, and is subsequently served with a technical assistance notice requiring access be provided to the agency's technical examiners.

Result: POTS is obliged to allow their systems to be assessed by the technical expert. However, after conducting this assessment the agency's technical examiners conclude that further assistance is not 'technically feasible' because no method of access can be devised that would not create a backdoor and thereby damage the platform's security for all users. As backdoors are prevented by a legal prohibition, agencies will be unable to conduct surveillance of communications on the POTS platform.

Business impact: While POTS cannot be required – or asked – to weaken its security or introduce a backdoor into its platform, it is required to comply with requests for technical information and systems access under a technical assistance notice.

Sunlite – a start-up

New technologies developed by small teams operating as start-ups can create entirely new challenges for law enforcement and intelligence agencies. Industry assistance aims to offer an approach to cooperation with the same level of agility as the start-ups themselves.

Company background: Taking advantage of trends in rooftop solar and home battery storage, a new start-up launches an Ethereum-based cryptocurrency platform for trading solar energy credits. Named Sunlite, the company raised $3 million for future development with an Initial Coin Offering that pegged the value of 1 kWh of Sunlite tokens to $1.50.

Problem: Because trades on the public Sunchain – Sunlite's ledger of transactions – can occur anonymously, and market fluctuations rapidly change the value of tokens, Sunlite has the unintended consequence of preventing energy retailers from accurately calculating power usage statistics. This allows criminal groups growing commercial quantities of marijuana in 'growhouses' to conceal the excess power use from their lighting rigs – often a red-flag for law enforcement.

Action: Detectives contact Sunlite's chief executive, Abigail, regarding the possibility of assistance to track Sunlite tokens used to purchase power for a suspected growhouse. Abigail suggests this is possible and that Sunlite is willing to help. Sunlite is issued with a technical assistance request that asks for the power purchased by IP addresses connected with the criminal group to be calculated – leaving the method to the provider's discretion.

Result: Once Abigail identifies the Sunlite wallet connected with the IP addresses she is able to easily calculate the amount of energy purchased by comparing the transactions to their point-in-time market value. Based on these estimates, the detectives are able to form reasonable suspicion required to obtain a search warrant for the premises.

Business impact: By working with authorities, Sunlite hopes to prevent its tokens becoming 'tainted' – having been purchased from the proceeds of crime – and being subject to potential lawful seizure. Sunlite and its employees are not subject to any civil liability for their actions to comply with the technical assistance request and Sunlite is compensated on terms negotiated with the agency. While the use of a technical assistance request must not be disclosed under non-disclosure rules, Sunlite may apply to the detectives' agency to make a disclosure of the assistance they have provided.