8 March 2022

Department of Home Affairs

Via Submission Link

Submission to the Department of Home Affairs regarding Reform of Australia's electronic surveillance framework discussion paper

About this submission

This submission is made to respond to certain targeted questions listed in the Electronic Surveillance Reform Discussion Paper. We welcome the opportunity to make a submission and we would like to thank the Department of Home Affairs for accepting this submission to the public consultation process concerning potential reforms to Australia's electronic surveillance framework.

The submission focuses on a selected number of questions relevant to data privacy, data governance and emerging technology instead of attempting to address all the sections listed in the discussion paper. We endorse the Department of Home Affairs' initiative to modernise the electronic surveillance legislations in light of emerging technologies.

Communications: What does this mean in 2021 and beyond?

5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?

The reform aims to replace the outdated concept of 'communications' with a term and definition that reflects the range of information and data transmitted electronically. We endorse this initiative to modernise the definition of communications and the proposal to keep the definition as technology-neutral as possible so that it can apply to future information and communications technologies. We agree that this will ensure the full range of information and data transmitted electronically is protected from unauthorised access and it will provide better protection from a data governance and privacy perspective.

Section 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth) defines communications as including (but not being limited to) a 'conversation and a message'. This can be in the form of speech, music or other sounds, data, text, visual images, signals or any other form or combination of forms.

This definition focuses on a conversation and a message in the setting of an interaction, when a communication can be made in the form of giving someone else access to certain information. Instead of creating a conversation or a message for the recipient, a person may give the recipient access to already created information, or disclose details in a recipient-controlled environment to enable interactions.

Some examples may include:

- Creation and storage of documents on a private server and provision of access to limited individuals
- Engaging in certain activities within an application that allows a user to interact with another user or share information with another user (e.g. in-game posts, in-game responses using pre-texted emoji, creation of a party or vending spot using certain titles)
- Giving another person or company access to opinions or information related to a person e.g. sharing GPS / location or health information with another user or company, responses to surveys

We recommend that the new definition of *Communication* should take into account such situations, and we propose the following definition*:*

> Any information generated by a person, an organisation or a machine that may potentially be disclosed to or accessed by another person, organisation or machine other than the creator of the information. This can be in the form of speech, music or other sounds, data, text, visual images, signals or any other form or combination of forms, and this also includes insights or analysis derived from the original information.

7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

Emerging technologies can generate new insights about a person but such analysis is still based on raw information gathered from a particular person. This is why we recommend adding “this also includes insights or analysis derived from the original information” to the definition of the communication.

Is there a real difference between ‘live’ and ‘stored’ communications anymore?

11. Should the distinction between ‘live’ and ‘stored’ communications be maintained in the new framework?

It is true that the line gets blurred when situations arise that a piece of information may be both live and stored. A text message could be intercepted while being transmitted or accessed after it is delivered and while it is stored on a provider’s systems or person’s device.

For law enforcement agencies, the threshold for intercepting live communications is higher than the threshold for accessing stored communications. And it is a good threshold to upload as intercepting live messages imposes greater privacy risks on the person being surveilled. It may also be required for a warrant to specify intercepting a transmitting message as it may require more advanced technology to perform such interception.

The term *live* imposes certain confusions as a piece of information may be stored but being played live. We recommend describing the current state of the information and distinguish the two states as *Transmitting* and *Stored*. If a piece of information is currently stored in an environment, including a vault, a physical server or a cloud application, the information should be considered *stored*. If the information is in transit from one environment to another, e.g. a phone call between two individuals, a chat message sending across servers, an email leaving from one server to another, the information will be considered *transmitting*. For emails messages, there will be seconds between an email leaving the originating server and arriving on the receiving server. All routing activities on the interim servers should be considered transmitting.

In the text message example above, if the government agency intends to intercept the message before it arrives on the recipient phone, it will be an attempt to capture a transmitting text message. If the government agency intends to intercept the message stored on the recipient's device, it will be an attempt to capture a stored message.

12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?

The privacy intrusion may impose different levels of privacy intrusion depending on the nature of the information collection. When intercepting transmitting information e.g. a phone conversation, the interceptor will not be able to predict what information may be shared and the conversation may include irrelevant portions intruding into irrelevant individuals' privacy.

When gathering information from a stored location, it is more likely that searches or reviews will help to narrow the scope to the current relevant proceeding.

This is also why we consider it important to maintain the differences between transmitting information and stored information, as intercepting the transmitting information may impose a greater privacy intrusion of individuals.

Consultation

Please contact us if you would like to discuss any aspect of this submission either in person or as a round table discussion.

Yours sincerely,

Shengshi Zhao

Director

Sentre Consulting

The authors' contribution is made in their personal capacity and does not necessarily represent the views of the author's employer, clients or workplace.