Justice & International Mission
Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Centre for Theology and Ministry
29 College Crescent
Parkville Victoria
Australia, 3052
Telephone: +61-3-9340 8807
jim@victas.uca.org.au

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
E-mail: pjcis@aph.gov.au

Supplementary Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into the mandatory data retention regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*
24 February 2020

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a supplementary submission to the mandatory data retention regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*. The Synod remains supportive of metadata retention, as a vital instrument in the fight against online child sexual abuse and other serious human rights abuses.

Recommendations

The Synod requests that the Committee makes the following recommendations:

- That the mandatory metadata retention period be increased to three years, to facilitate being able to identify further victims a human rights abuser has harmed (such as a child sexual abuse offender who has a long history of abusing numerous children facilitated online), to assist in identifying others involved in serious criminal activities and human rights abuses;
- That the existing system of access to metadata by law enforcement agencies investigating serious crimes, many of which are also severe human rights abuses, be maintained while addressing the issues identified by the Commonwealth Ombudsman:
    - Establishing a formal framework for law enforcement agencies to verbally issue authorisations for access to telecommunications data in urgent out-of-hours cases;
    - Formal procedures around the storage of telecommunications data obtained by law enforcement agencies;
    - Formal procedures for the destruction of telecommunications data obtained by law enforcement agencies and for length of retention before destruction;
    - Clarification on what constitutes 'content'; and
    - Clarification on when revocation of an authorisation takes effect.
- There be no introduction of measures that will tip-off suspected offenders they are under investigation. There is a need to avoid tipping off suspected offenders to prevent them being able to destroy evidence (both in the physical world and across multiple platforms), tip-off other offenders, intimidate victims and witnesses or seek to bribe the family of a child sexual abuse victim to not co-operate in an investigation. These are all activities that some child sexual abuse offenders will undertake if given early warning of an investigation, such as being tipped off that a warrant has been applied for. Child sexual abuse offenders often

collaborate in large online networks, assisted by the anonymity that the online world provides them.

- That the government evaluate the benefits and risks of allowing law enforcement agencies to more rapidly access content through an emergency process where there is an immediate threat to lives or where a person is in immediate danger of on-going serious harm, such as children being sold for rape, torture and sexual abuse via live webcam. When a child is being subjected to daily rape or sexual abuse facilitated online, it is vital that law enforcement as able to locate and rescue the child as soon as possible. It is completely unacceptable to place unnecessary obstructions and delays in the way of law enforcement being able to rescue the child from on-going abuse.
- That there needs to be a review of the *Public Interest Disclosure Act 2013* to determine if the Parliament believes that section 26 needs to be amended to increase the circumstances in which a public servant can make external disclosures to journalists of confidential information without the public servant or the journalist being investigated for a breach of the law. It makes no sense to make certain disclosures by public servants to journalists illegal, but then forbid the Australian Federal Police or other law enforcement agencies from being able to investigate the illegal disclosure. It would make more sense to simply make certain disclosures legal. However, it will probably be impossible to eliminate cases in which the public servant and the journalist will argue they have not breached the law and the government of the day will argue they have. In such cases, it is likely the Australian Federal Police might still decide to investigate to determine if the disclosure is in accordance with the protections provided by the *Public Interest Disclosure Act 2013*. While it is understandable that media corporations would rather have the certainty that all leaks from public servants to media outlets are not able to be investigated by law enforcement agencies, it should be the Parliament that decides which disclosures from public servants to journalists are lawful and in what circumstances.

To gain a better understanding of what telecommunications data the US law enforcement agencies are able to access and under what circumstances, the Committee should seek a briefing from the FBI which could be facilitated by the FBI agents based in the US Embassy in Canberra.

Key points

- Access to metadata allows law enforcement agencies to:
    - Locate and rescue children from on-going rape, torture and sexual abuse;
    - Eliminate suspects in serious crimes like murder;
    - Identify victims of serious crimes, many of which are also serious human rights abuses, to rescue them from further abuse or provide them with support;
    - Identify suspects in serious crimes, many of which are human rights abuses as well;
    - Build up knowledge of criminal networks and organisations and how they are operating and recruiting;
    - Identity lines of investigation to gather evidence to prevent further serious crimes, many of which are human rights abuses; and
    - Provide courts with evidence of the extent of an offender's activities, which is an important factor in considering the severity of the offending when it comes to sentencing.

- The longer the length data is stored increases the ability of law enforcement agencies to achieve the above outcomes. The Synod accepts this needs to be weighed against the additional costs of storage given the volume of metadata generated.
- It is the Parliament that should determine what data law enforcement agencies should have access to and under what circumstances. Technology companies should not be given the ability to obstruct or hinder lawful investigations by law enforcement agencies.
- It is the Parliament that should set the laws under which public servants can lawfully disclose confidential information to journalists and the courts to decide if a disclosure has been lawful when it is disputed. It should not be for journalists and media corporations to decide what confidential information it is acceptable for public servants to leak.
- Any additional impediments to law enforcement access to metadata will reduce the number of cases that law enforcement can conduct, meaning fewer victims rescued from on-going serious harm, and there is a further erosion of general deterrence. General deterrence is eroded when law enforcement agencies are subjected to restrictions and impediments that increase the perception amongst offenders that they will be able to get away with the harm they are inflicting on others. Reducing the number of cases law enforcement agencies are able to work on will legitimately increase the perception that there is less risk of being caught and sanctioned.
- There is no evidence that has been presented to the Committee that Australian law enforcement agencies have misused access to metadata to engage in malicious prosecution or other malicious activities that have caused harm to any person. The cases highlighted by the Commonwealth Ombudsman are of law enforcement agencies failing to follow the required procedures while conducting legitimate investigations into criminal or unlawful activity. There may be questions about why certain investigations have been prioritised, such as those involving public servants providing confidential information to journalists. However, if there is a problem here, the solution is to make the activities in question lawful, so that police have no reason to conduct an investigation. For example, by increasing the circumstances in which public servants are lawfully able to disclose confidential information to journalists. There is, therefore, no justification for restricting law enforcement agencies to access stored metadata based on these cases. While law enforcement agencies must make decisions about how they use their resources and what priorities they set, it would be very dangerous to allow law enforcement agencies to usurp the role of the elected Parliament by deciding they do not like certain laws and therefore will not enforce them. Balanced against law enforcement agencies deciding not to enforce certain laws is the community pressure that is applied to law enforcement agencies when they enforce unpopular laws.
- By contrast, the harm caused by impeding law enforcement agencies access to metadata and reducing the amount of metadata retained will be more children subjected to rape, torture and other sexual abuse for longer and more serious crimes that cause real harm to people being unable to be investigated. Impeding access to metadata means that for the same level of law enforcement resources, fewer cases can be investigated. Increasing the role of courts in having to issue warrants would take up more time before the courts and is likely to further impede law enforcement investigations as there are further delays in the issuing of warrants. As noted below, media reports state that it can take police up to a month in Canada to just get a warrant for basic subscriber data (who a suspect is) in cases of online child sexual abuse. That is a long time to leave a child at the mercy of an abuser. The Synod would have preferred to check the accuracy of these media reports with the Royal Canadian Mounted Police if time had permitted.

- The table below compares the harms. Given the gulf in the seriousness of harm between the harm from impeding law enforcement investigations against the 'harm' of law enforcement agencies not following procedure to access metadata, the onus should fall on those seeking to restrict metadata retention and access to provide evidence to the Committee about the extent to which such restrictions will result in an increase in severe human rights abuses and serious criminal activity and why that increase is an acceptable outcome. However, those seeking to restrict access to metadata and reduce its retention have failed to show the Committee they have given these concerns any meaningful attention or consideration.

Table comparing harms based on possible Committee recommendations.

Worst case outcomes of Committee recommending a reduction in the length of metadata retention and it being implemented	**Worst case outcomes if the Committee recommends an increase in the length of mandatory metadata retention and it is implemented**
• Victims outside of the metadata retention period are not identified. • Networks of offenders outside of the retention period are not identified. • Offenders receive lesser sanctions for serious harms they have caused as the court is unable to be presented with the offender's full history of harms inflicted.	• Increased cost to the businesses that need to store the metadata. • There is a risk that stored metadata will be hacked, but it is unclear the degree to which historical metadata is useful to criminals.
Worst case outcomes of the Committee recommending law enforcement agencies need to obtain a court-issued warrant every time they wish to access stored metadata.	**Worst case outcomes of the Committee recommending law enforcement agencies continue to be able to authorise access to metadata for serious crime investigations under the existing regime.**
• Law enforcement agencies are able to identify and rescue fewer victims of rape, torture, sexual assault and other serious human rights abuses. • Delays in issuing warrants delay the rescue of children from on-going rape and sexual assault in situations like live webcam streaming of such abuse. • Law enforcement agencies are able to prevent fewer crimes from taking place, resulting in serious human rights abuses and harms. • More government revenue is stolen through fraud and tax evasion.	• Law enforcement agencies continue to make administrative errors in accessing metadata, resulting in them not properly accessing metadata needed for criminal investigations. • Law enforcement agencies pursue public servant whistleblowers and journalists to prevent public disclosures lawfully permitted under the *Public Interest Disclosure Act* by creating an atmosphere of fear of prosecution for legitimate whistleblower actions.
Worst case outcomes if the Committee recommends that law enforcement agencies no longer are able to access location data as part of stored metadata and the measure is implemented.	

• Law enforcement agencies have greater difficulty locating and rescuing children being subjected to on-going rape and sexual abuse. • Law enforcement agencies have greater difficulty locating missing persons. • Law enforcement agencies are no longer able to eliminate suspects to a serious crime based on their location at the time of the crime.	

- The key arguments for the Committee to recommend a reduction in the length of mandatory retention of metadata are that other jurisdictions have done so, there are costs to businesses that need to store the metadata and assist law enforcement agencies, and some courts have prioritised the right to privacy over the rights of people not to be subjected to cruel, degrading and inhumane treatment and the duty of governments under human rights treaties to prevent the sexual abuse and exploitation of children. Simply because other governments have prioritised the right to privacy over the right of children not to be subjected to child sexual abuse and exploitation (through reducing the effectiveness and capability of their law enforcement agencies to detect and prevent such abuses) is a poor reason for the Australian Parliament to make the same decision.
- The Committee no doubt recognises that it is difficult for law enforcement agencies to have to defend their access to investigative tools publicly. They have legitimate concerns that criminals and human rights abusers will use publicly disclosed information to alter their behaviour to make detection of their criminal activities more difficult. At the same time, there is an understandable desire for some in the community for law enforcement agencies to have to justify the powers they have been granted.
- There are many areas where the Australian Parliament and governments need to balance the right to privacy against other human rights that protect people from serious harms that themselves are human rights abuses. As stated before the Committee, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* requires reporting entities to have in place systems that detect suspicious patterns of transactions across all transactions for all customers. Any suspicious patterns must be reported to AUSTRAC. Clearly, the Parliament decided that the need to protect the community from the serious harms that generate profits to be laundered justified the impacts on the right to privacy in relation to financial transactions. Under this Act, transaction records must be kept for seven years.[1] As another example, some police vehicles in Australia are fitted with Automatic Number Plate Recognition, that allows police to scan number plates to identify unlicensed drivers, unregistered or stolen vehicles, drivers with interlock conditions and motorists with outstanding warrants.[2] State Parliaments have decided that it is not necessary for police to have to get a court-issued warrant every time they wish to check the registration details of a vehicle. Registration details of a vehicle are not dissimilar to subscriber data for an online account. The Committee may wish to consider what are the reasons why data around online communication and activity should be treated differently to financial transaction data when it comes to balancing the human rights of people to be protected from serious harm against

[1] https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/record-keeping
[2] Victorian Minister for Police and Emergency Services Lisa Neville, 'High-Tech Tool To Target Dangerous Drivers', Media Release, 13 February 2019.

the right to privacy. The Synod is concerned that the existing culture that the online world is a largely unregulated place is having an undue influence on the public discussion of the need to balance the different human rights obligations that the Australian Government has.

Impeding access to metadata reduces the number of cases police can investigate

As stated before the Committee, throwing up additional barriers to law enforcement access to metadata will reduce the number of cases that law enforcement can deal with. The Australian Federal Police already have many more cases of child sexual abuse online than they have the resources to deal with. Impeding these investigations by greater restrictions on access to metadata, such as a court-issued warrant, will mean fewer children rescued from on-going abuse. The reduction in the number of cases where children are protected from further sexual abuse has already been demonstrated by Canada. In Canada, police are now required to obtain a judicial authorisation signed by a judge to have an Internet Service Provider tell the police the identity of people using their service. The requirement has significantly reduced the number of cases of online child sexual abuse that Canadian police are able to investigate.[3] As noted in the Canadian media, previously Internet Service Providers were required by law to notify the Canadian Centre for Child Protection when child sexual abuse material was shared.[4] The Centre then provided the IP address to law enforcement agencies. In 2011, a change in Canadian law gave police investigators easy access to the subscriber records of ISPs to obtain the name and address of the person associated with an IP at the relevant point in time. In 2014, the Supreme Court of Canada ruled that police were required to have a search warrant to get the name and address of a person associated with an IP address.[5] Police can now have to wait up to a month to get the warrant.[6] A child sex offender may engage in over a hundred sessions of live webcam sexual abuse in a month. As noted by Canadian media, hundreds or thousands of cases of child sexual abuse online now go uninvestigated in Alberta and Ontario alone.[7] The Committee should seek to avoid making recommendations that will unnecessarily expose children to on-going sexual abuse by denying police prompt access to be able to identify and further investigate those engaged in such horrific abuse. This also demonstrates the vital role that maintaining metadata plays in the struggle to curb online child sexual abuse.

In the 2014 case considered by the Supreme Court of Canada, the offender had downloaded child sexual abuse material and placed it in a folder accessible to other Internet users using the same file-sharing program.[8] Being able to identify the offender from their IP address allowed the police to apprehend the offender who was subsequently convicted at trial of possession of child

[3] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5.
[4] Michael Mui, 'Police overwhelmed by rampant, 'hidden evil' of child exploitation online', *The Star,* 2 February 2019, https://www.thestar.com/news/canada/2019/02/02/police-overwhelmed-by-rampant-hidden-evil-of-child-exploitation-online.html
[5] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[6] Michael Mui, 'Police overwhelmed by rampant, 'hidden evil' of child exploitation online', *The Star,* 2 February 2019, https://www.thestar.com/news/canada/2019/02/02/police-overwhelmed-by-rampant-hidden-evil-of-child-exploitation-online.html
[7] Michael Mui, 'Police overwhelmed by rampant, 'hidden evil' of child exploitation online', *The Star,* 2 February 2019, https://www.thestar.com/news/canada/2019/02/02/police-overwhelmed-by-rampant-hidden-evil-of-child-exploitation-online.html
[8] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

sexual abuse material and acquitted on a charge of making it available.[9] In the appeal the defence team did not argue that the defendant did not access child sexual abuse material, but rather he had a right to expect the ISP would conceal his identity from police as part of his right to privacy.[10] The Synod strongly urges the Committee to reject the absurdity of such an argument. The right to privacy should not be a right to have a shield against being held to account for committing serious human rights abuses. However, the Supreme Court of Canada did rule that a person engaged in online child sexual abuse should have a reasonable expectation of privacy in their subscriber information and that a police request for an ISP to voluntarily disclose such information amounted to a search.[11] Fortunately, the court dismissed the appeal and upheld the conviction. The court ruled that while the police should have obtained a warrant to access the offender's subscriber data to identify him, police had acted in good faith and the administration of justice would be impaired if the broader evidence gathered by police were thrown out of court.[12] The Synod position is that such requests from police should be by a warrant that compels the subscriber information, without the warrant needing to be issued by a court that would impede the further investigation. A court-issued warrant should be required at the point where police wish to access the content of the alleged offender's online activity. However, even here, where there is an immediate threat to lives or to a person being subjected to on-going serious human rights violations, there is a case to be made for processes that allow for rapid access to necessary data by law enforcement agencies.

The Virtual Global Taskforce reported that a joint report between Online Child Exploitation Across New Zealand (OCEANZ) and the New Zealand Police, *Online Child Exploitation: Emerging Trends and the Pacific. Intelligence Report,* reported that data preservation and data retention created challenges to investigations into online child sexual abuse due to the data retention practices and policies of ISPs.[13] The Synod has been unable to locate a publicly available copy of the report.

The Virtual Global Taskforce also reported that investigations into online child sexual abuse were being impeded by ISPs failing to comply with legislative obligations.[14]

[9] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[10] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[11] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[12] CBC News, 'Internet users' privacy upheld by Canada's top court', 14 June 2014.
[13] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 25.
[14] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 25.

Justice & International Mission
Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

US legal regime for access to metadata.

It was suggested to the Committee by other witnesses that US law enforcement agencies are not able to access metadata without a court-issued warrant. That information is incorrect. The Synod acknowledges that the US legal system is far more complex than the Australian legal system. In the time that has been available since the hearing, the Synod has identified the following relevant information. If the Committee wishes to explore if Australia should more closely align its regime for the access to metadata to the US regime, the Synod would strongly urge the Committee to seek a briefing from the FBI. Arranging for such a briefing may be possible through the FBI agents stationed in the US Embassy in Canberra.

US law enforcement agencies are able to access metadata for certain types of serious crime through being able to issue administrative subpoenas without the approval of a court under 18 US Code § 3486. Administrative subpoenas, which states:

> *(a)Authorization.—*
> *(1) (A)In any investigation of—*
>
> *(i) (I)a Federal health care offence; or*
> *(II) a Federal offence involving the sexual exploitation or abuse of children, the Attorney General;*
>
> *(ii)an unregistered sex offender conducted by the United States Marshals Service, the Director of the United States Marshals Service; or*
>
> *(iii)an offence under section 871 or 879, or a threat against a person protected by the United States Secret Service under paragraph (5) or (6) of section 3056,[1] if the Director of the Secret Service determines that the threat constituting the offence or the threat against the person protected is imminent, the Secretary of the Treasury,*
> *may issue in writing and cause to be served a subpoena requiring the production and testimony described in subparagraph (B).*
>
> *(B)Except as provided in subparagraph (C), a subpoena issued under subparagraph (A) may require—*
> *(i)the production of any records or other things relevant to the investigation; and*
> *(ii)testimony by the custodian of the things required to be produced concerning the production and authenticity of those things.*
>
> *(C) A subpoena issued under subparagraph (A) with respect to a provider of electronic communication service or remote computing service, in an investigation of a Federal offence involving the sexual exploitation or abuse of children shall not extend beyond—*
>
> *(i) requiring that provider to disclose the information specified in section 2703(c)(2), which may be relevant to an authorized law enforcement inquiry; or*
> *(ii) requiring a custodian of the records of that provider to give testimony concerning the production and authentication of such records or information.*
>
> *(D)As used in this paragraph—*
> *(i)the term "Federal offence involving the sexual exploitation or abuse of children" means an offence under section 1201, 1591, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A,*

2260, 2421, 2422, or 2423, in which the victim is an individual who has not attained the age of 18 years; and
(ii)the term "sex offender" means an individual required to register under the Sex Offender Registration and Notification Act (42 U.S.C. 16901 et seq.).[2]

(2) A subpoena under this subsection shall describe the objects required to be produced and prescribe a return date within a reasonable period of time within which the objects can be assembled and made available.

(3) The production of records relating to a Federal health care offence shall not be required under this section at any place more than 500 miles distant from the place where the subpoena for the production of such records is served. The production of things in any other case may be required from any place within the United States or subject to the laws or jurisdiction of the United States.

(4) Witnesses subpoenaed under this section shall be paid the same fees and mileage that are paid witnesses in the courts of the United States.

(5) At any time before the return date specified in the summons, the person or entity summoned may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the summons, or a prohibition of disclosure ordered by a court under paragraph (6).

(6) (A)A United States district court for the district in which the summons is or will be served, upon application of the United States, may issue an ex parte order that no person or entity disclose to any other person or entity (other than to an attorney in order to obtain legal advice) the existence of such summons for a period of up to 90 days.
(B)Such order may be issued on a showing that the things being sought may be relevant to the investigation and there is reason to believe that such disclosure may result in—
(i)endangerment to the life or physical safety of any person;
(ii)flight to avoid prosecution;
(iii)destruction of or tampering with evidence; or
(iv)intimidation of potential witnesses.
(C)An order under this paragraph may be renewed for additional periods of up to 90 days upon a showing that the circumstances described in subparagraph (B) continue to exist.

(7) A summons issued under this section shall not require the production of anything that would be protected from production under the standards applicable to a subpoena duces tecum issued by a court of the United States.

(8) If no case or proceeding arises from the production of records or other things pursuant to this section within a reasonable time after those records or things are produced, the agency to which those records or things were delivered shall, upon written demand made by the person producing those records or things, return them to that person, except where the production required was only of copies rather than originals.

(9) A subpoena issued under paragraph (1)(A)(i)(II) or (1)(A)(iii) may require production as soon as possible, but in no event less than 24 hours after service of the subpoena.

(10) As soon as practicable following the issuance of a subpoena under paragraph (1)(A)(iii), the Secretary of the Treasury shall notify the Attorney General of its issuance.
(b) Service.— A subpoena issued under this section may be served by any person who is at least 18 years of age and is designated in the subpoena to serve it. Service upon a natural person may be made by personal delivery of the subpoena to him. Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name, by delivering the subpoena to an officer, to a managing or general agent, or to any other agent authorized by appointment or by law to receive service of process. The affidavit of the person serving the subpoena entered on a true copy thereof by the person serving it shall be proof of service.
(c) Enforcement.— In the case of contumacy by or refusal to obey a subpoena issued to any person, the Attorney General may invoke the aid of any court of the United States within the jurisdiction of which the investigation is carried on or of which the subpoenaed person is an inhabitant, or in which he carries on business or may be found, to compel compliance with the subpoena. The court may issue an order requiring the subpoenaed person to appear before the Attorney General to produce records, if so ordered, or to give testimony concerning the production and authentication of such records. Any failure to obey the order of the court may be punished by the court as a contempt thereof. All process in any such case may be served in any judicial district in which such person may be found.
(d) Immunity From Civil Liability.— Notwithstanding any Federal, State, or local law, any person, including officers, agents, and employees, receiving a subpoena under this section, who complies in good faith with the subpoena and thus produces the materials sought, shall not be liable in any court of any State or the United States to any customer or other person for such production or for nondisclosure of that production to the customer.
(e) Limitation on Use.—
(1) Health information about an individual that is disclosed under this section may not be used in, or disclosed to any person for use in, any administrative, civil, or criminal action or investigation directed against the individual who is the subject of the information unless the action or investigation arises out of and is directly related to receipt of health care or payment for health care or action involving a fraudulent claim related to health; or if authorized by an appropriate order of a court of competent jurisdiction, granted after application showing good cause therefor.
(2) In assessing good cause, the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services.
(3) Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.

The Synod prefers the Australian system as the crime types caught under the US administrative subpoena system do not seem to have any particularly obvious logic to why these serious crimes were included and not others.

18 US Code § 2703(c)(2) Required disclosure of customer communications or records, states:

(2)A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
(A) name;
(B) address;
(C) local and long distance telephone connection records, or records of session times and durations;
(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

As noted by the US Department of Justice, access to the information specified in 18 US Code § 2703(c)(2) may be obtained using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. For example, subpoenas authorized by the *Inspector General Act* may be used.[15]

Subpoenas for metadata can also be issued under 28 US Code § 1782.Assistance to foreign and international tribunals and to litigants before such tribunals:

(a)The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation. The order may be made pursuant to a letter rogatory issued, or request made, by a foreign or international tribunal or upon the application of any interested person and may direct that the testimony or statement be given, or the document or other thing be produced, before a person appointed by the court. By virtue of his appointment, the person appointed has power to administer any necessary oath and take the testimony or statement. The order may prescribe the practice and procedure, which may be in whole or part the practice and procedure of the foreign country or the international tribunal, for taking the testimony or statement or producing the document or other thing. To the extent that the order does not prescribe otherwise, the testimony or statement shall be taken, and the document or other thing produced, in accordance with the Federal Rules of Civil Procedure.
A person may not be compelled to give his testimony or statement or to produce a document or other thing in violation of any legally applicable privilege.

(b)This chapter does not preclude a person within the United States from voluntarily giving his testimony or statement, or producing a document or other thing, for use in a proceeding in a foreign or international tribunal before any person and in any manner acceptable to him.

It is our understanding under the above section once a person is authorized by the court they may issue subpoenas without needing further court approval for the subpoena to access metadata.

[15] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 128-129. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

US law enforcement agencies can also obtain data in exigent circumstances. These are when:[16]
1. Evidence is in imminent danger of destruction;
2. A threat puts either the police or the public in danger;
3. The police are in "hot pursuit" of a suspect; or
4. The suspect is likely to flee before the officer can secure a search warrant.

In *United States v. Gorshkov*, 2001 WL 1024026, at *4 (W.D. Wash. 23 May 2001) law enforcement officers downloaded content, not just metadata, from a computer in Russia without a warrant. They were permitted to do so because probable cause existed to believe that the Russian computer contained evidence of a crime and there was good reason to fear that delay could lead to the destruction of or loss of access to evidence. The agent copied the data and subsequently obtained a search warrant.[17]

US law also allows for businesses to voluntarily disclose both metadata and content data when the provider of the service is not available "to the public". For example, in the case of *Andersen Consulting LLP v. UOP,* 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting. Andersen Consulting employees were given accounts on UOP's computer network. After the relationship between UOP and Andersen Consulting soured, UOP disclosed the emails of the Andersen Consulting employees on the UOP network to *The Wall Street Journal*. Andersen Consulting sued, claiming that the disclosure of the email contents by the provider had violated the *Stored Communications Act*. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public.[18]

In addition, under the US legal system, there is the complexity of state laws that seek to restrain the operation of the Federal laws. An example is the 2015 *California Electronic Communications Privacy Act* (CalECPA). CalECPA specifically bars state law enforcement and other investigative agencies from compelling a California business or other entity that possesses a third-party's metadata or digital communications to turn over that information without a warrant or court order. Under CalECPA, the entity that executes a search warrant of a third party must provide contemporaneous notice to the identified target, which must inform the target that information about them has been requested and must state the nature of the government investigation under which the information is sought. However, this can be delayed for 90 days (which can be renewed).[19] The Committee could investigate what impact these tipping off provisions have had on the ability of Californian law enforcement officers to conduct investigations while avoiding the ability of offenders to destroy evidence.

---

[16] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 27-28. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[17] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 29. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[18] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 135. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[19] Proskauer Privacy Law Blog, "California Gives the Fourth Amendment a 21st Century Makeover", 10 November 2015. https://privacylaw.proskauer.com/2015/11/articles/fourth-amendment/california-gives-the-fourth-amendment-a-21st-century-makeover/ accessed 20 February 2020.

Under CalECPA, a warrant is not required in emergencies when accessing the data or tracking an electronic storage device could prevent loss of life or physical injury.[20]

The multiple layers of US legislation regulating government access to electronic communications have led to a somewhat confusing legal framework, which has been additionally complicated by key court decisions – including lower court decisions. In order to provide some clarity for federal law enforcement officials, the US Department of Justice publishes a guide titled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.[21] The latest version of this guide (as at February 2020) is the third edition published in 2009.

In 2014 ProPublica, an investigative journalism non-profit organisation published a detailed list of how law enforcement can gain access without a warrant showing probable cause. Many of the examples given by ProPublica relate to metadata, but some related to items such as emails and texts more than 180 days old. Full details are set out in the table below. The information below dates from 2014, so some legal provisions may have changed, and the table notes in some places that at time of publication there were bills before Congress designed to introduce changes.[22]

ProPublica summary of government access to private data without a warrant showing probable cause		
Data to be accessed	**How law enforcement access it**	**What the law says**
PHONE RECORDS Who was called and when	Listening to phone calls without a judge's warrant is illegal if you're a US citizen. Police don't need a warrant — which requires showing "probable cause" of a crime— to monitor the numbers for incoming and outgoing calls in real-time, as well as the duration of the calls. Instead, they can get a court to sign off on an order that only requires the data they're after is "relevant to an ongoing criminal investigation"— a lesser standard of evidence. The	Police can get phone records without a warrant as a result of a 1979 Supreme Court case, *Smith v. Maryland*, which found that the Constitution's Fourth Amendment protection against unreasonable search and seizure doesn't apply to a list of phone numbers. The *Electronic Communications Privacy Act* (ECPA)1986 requires providers to allow access to real-time data with a court order and historical data with a subpoena that does

[20] Proskauer Privacy Law Blog, "California Gives the Fourth Amendment a 21st Century Makeover", 10 November 2015. https://privacylaw.proskauer.com/2015/11/articles/fourth-amendment/california-gives-the-fourth-amendment-a-21st-century-makeover/ accessed 20 February 2020.
[21] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf accessed 19 February 2020.
[22] ProPublica, "No Warrant, No Problem: How the Government Can Get Your Digital Data", 27 June 2014. https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data accessed 21 February 2020.

	government can also get historical phone records with an administrative subpoena, which doesn't require a judge's approval.	not need court approval.
LOCATION DATA	Many cell phone carriers provide authorities with a phone's location and may charge a fee for doing so. Cell towers track where a phone is at any moment; so can the GPS features in some smartphones. In response to an inquiry by Senator Edward J. Markey, a Massachusetts Democrat, Sprint reported that it provided location data to US law enforcement 67,000 times in 2012. AT&T reported receiving 77,800 requests for location data in 2012. (AT&T also said that it charges $100 to start tracking a phone and $25 a day to keep tracking it.) Other carriers, including T-Mobile, U.S. Cellular and Verizon, didn't specify the number of location data requests they had received or the number of times they've provided it. Internet service providers can also provide location data that tracks users via their computer's IP address.	Courts have been divided for years on whether police need a warrant from a judge to get cell phone location data. In 2005, Judge Stephen W. Smith denied a government request for real-time access to location data, and some judges have followed his lead. But other courts have ruled that no warrant is necessary. Authorities only have to show that, under the ECPA, the data contains "specific and articulable facts" related to an investigation, a lesser standard than probable cause. Montana, Maine, Wisconsin, Utah and Colorado have passed laws requiring police to get a warrant for location data in most circumstances. Recent court rulings have created a patchwork of rules depending on where a person lives and who's requesting the data. New Jersey's Supreme Court ruled in 2013 that police needed a warrant to get real-time location data, and Massachusetts' Supreme Judicial Court ruled in February 2014 that authorities needed a warrant to get historical location data for significant periods of time. But those decisions apply only to state authorities in those states, not federal law enforcement agencies like the FBI.

		Federal appeals courts have split on whether police can get historical location data from cell carriers without a warrant. The Fifth Circuit in New Orleans ruled in 2013 that police don't need a warrant, while the 11th Circuit in Atlanta ruled in 2014 that they do. The rulings mean that police in the 11th Circuit — which covers Alabama, Georgia and Florida — need to get a warrant for location data, while authorities in the Fifth Circuit — Texas, Louisiana and Mississippi — don't need to do so.
IP ADDRESSES	The standard for IP addresses is the same as the one for phone records: Authorities can get a court order allowing real-time access as long the court approves that the records are relevant to an investigation. They can also get historical records of IP addresses with an administrative subpoena.	In the 2007 *U.S. v. Forrester*, a case involving two men trying to set up a drug lab in California, the government successfully argued that tracking IP addresses was no different from installing a device to track every telephone number dialled by a given phone (which is legal).
EMAILS	Authorities need a warrant to get unopened emails that are less than 180 days old, but they can obtain opened email as well as unopened emails that are at least 180 days old with only a subpoena as long as they notify the customer whose email they've requested. The government can also get older unopened emails without notifying the customer if they get a court order that requires them to offer "specific and articulable facts showing	In *U.S. v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit ruled in 2010 that authorities should have gotten a search warrant for the emails of Steven Warshak, a Cincinnati businessman convicted of wire fraud in which his emails were used as evidence. The decision only applies in the Sixth Circuit, which covers Michigan, Ohio, Kentucky and Tennessee, but it's had an influence beyond those states. Google, Microsoft

	that there are reasonable grounds to believe" the emails are "relevant and material to an ongoing criminal investigation" — a higher bar than a subpoena.	and Yahoo have said they refuse to turn over emails without a warrant and cited the ruling.
TEXT MESSAGES	Investigators need only a court order or a subpoena, not a warrant, to get text messages that are at least 180 days old from a cell provider — the same standard as emails. Many carriers charge authorities a fee to provide texts and other information. Sprint charged $30 for access to a customer's texts, according to documents obtained by the ACLU in 2012, while Verizon charged $50.	The ECPA also applies to text messages, which is why the rules are similar to those governing emails. But the ECPA doesn't apply when it comes to reading texts or accessing other data on a physical cell phone rather than getting them from a carrier. The Supreme Court ruled unanimously that police needed a warrant to search the phones of people who had been arrested.
CLOUD DATA	Authorities typically need only a court order or a subpoena to get data from Google Drive, Dropbox, SkyDrive and other services that allow users to store data on servers, or "in the cloud," as it's known.	The law treats cloud data the same as draft emails — authorities don't need a warrant to get it. But files that have been shared with others — say, a collaboration using Google Docs — might require a warrant under the ECPA if it's considered "communication" rather than stored data.
SOCIAL MEDIA	When it comes to sites like Facebook, Twitter and LinkedIn, the rules depend on what authorities are after. Content is treated the same way as emails — unopened content less than 180 days old requires a warrant, while opened content and content at least 180 days old does not. Authorities can get IP addresses from social networks the same way they get them from Internet Service Providers — with a court order showing the	Courts haven't issued a definitive ruling that distinguishes social media posts from other electronic communications. In 2012, a New York judge upheld a prosecutor's subpoena for information from Twitter about an Occupy Wall Street protester arrested on the Brooklyn Bridge. It was the first time a judge had allowed prosecutors to use a subpoena to get information from Twitter rather than forcing them to

	records are relevant to an investigation for real-time access, and with a subpoena for historical records. Twitter has reported that it received 1,494 requests for user information from U.S. authorities in 2012 and 1,735 requests in 2013. In the second half of 2013, Twitter reported that 55 per cent of the requests were from subpoenas, 7 per cent through other court orders, 26 per cent came through search warrants, and 12 per cent came through other ways. Twitter says that "non-public information about Twitter users is not released except as lawfully required by appropriate legal processes such as a subpoena, court order, or other valid legal processes, except in emergencies "involving the danger of death or serious physical injury to a person." Facebook said it requires a warrant from a judge to disclose a user's "messages, photos, videos, wall posts, and location information." But it will supply basic information, such as a user's email address or the IP addresses of the computers from which someone recently accessed an account, under a subpoena.	get a warrant.

Paedophile networks and the need to avoid tipping them off

Paedophiles often operate in large online networks that assist each other. Thus, the Committee should strongly avoid recommending any measures that would allow a suspected paedophile they are under investigation. Any process that would tip off a suspected paedophile may allow

them to destroy evidence as well as alert others in their network and possibly seek assistance from others in the network to cover up their activities. What follows is some brief evidence about such networks and how they operate. The Synod is able to provide further information to the Committee on such networks if it is needed.

As an example, *The Financial Times* reported that videos and images of children being sexually abused were openly shared on Facebook's WhatsApp on a vast scale by networks of paedophiles.[23] In one case, one of these groups had 256 members.

Cyber-psychologist Mary Aiken, who has assisted law enforcement agencies across the globe, reports that networks of paedophiles sometimes hunt in packs in online multiplayer games and will have a team they invite the child into where they pretend they do not know each other.[24] The child is then groomed by the team.

Networks of paedophiles have developed handbooks and manuals to assist each other. These handbooks are highly detailed and instructive in content.[25] They will contain advice on how to entrap or groom a child, where to find a child victim, how to offend and escape capture.[26] For example, in November 2018 a man was imprisoned in the UK who had in his possession five paedophile manuals, including a Harry Potter-inspired child sexual abuse manual.[27] He had a three-part manual which contained guidance on how to abuse children aged between five and eight. These include advice on how to have sex with a child 'safely', as well as how to win a child's obedience and cooperation. The 24-page manual, which used references taken from the Harry Potter series of books, contained technical guidance on how not to get caught by the police. In the US in 2018 a man was imprisoned for child sexual abuse offences who had in his possession a downloaded copy of the 576 page 'The Paedophile's Handbook'.[28] The handbook includes chapters such as "Finding Children" and "Hunting Season". One chapter offers help to readers to "learn the basics about how to find yourself children through various methods, and how to befriend them."[29] Another offered to help readers learn "how to stay secure as an active

[23] Leila Abboud, Hannah Kuchler and Mehul Srivastava, 'WhatsApp fails to curb sharing of child sex abuse videos', *The Financial Times,* 20 December 2018, https://www.ft.com/content/bff119b8-0424-11e9-99df-6183d3002ee1
[24] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 153.
[25] UK Ministry of Justice, 'Serious Crime Act 2015. Fact sheet: Offence of possession of paedophile manuals', March 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415982/Fact_sheet_-_Paedophile_manuals_-_Act.pdf
[26] UK Ministry of Justice, 'Serious Crime Act 2015. Fact sheet: Offence of possession of paedophile manuals', March 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415982/Fact_sheet_-_Paedophile_manuals_-_Act.pdf
[27] UK Crown Prosecution Service, 'Man jailed for possessing paedophile manuals', 5 November 2018, https://www.cps.gov.uk/london-north/news/man-jailed-possessing-paedophile-manuals
[28] 'Man With 'Pedophile's Handbook' Gets 37 Years For Making, Possessing Child Porn', 2 May 2018, https://www.nbcchicago.com/news/local/man-with-pedophiles-handbook-gets-37-years-for-making-possessing-child-porn/48474/
[29] 'Man With 'Pedophile's Handbook' Gets 37 Years For Making, Possessing Child Porn', 2 May 2018, https://www.nbcchicago.com/news/local/man-with-pedophiles-handbook-gets-37-years-for-making-possessing-child-porn/48474/

paedophile and how to handle civilians and police, even prisons, if things should go really wrong."[30]

Dr Mark Zirnsak
Senior Social Justice Advocate
[redacted]

[30] 'Man With 'Pedophile's Handbook' Gets 37 Years For Making, Possessing Child Porn', 2 May 2018, https://www.nbcchicago.com/news/local/man-with-pedophiles-handbook-gets-37-years-for-making-possessing-child-porn/48474/