Helsinki Information Law Moot Court 2023 Problem

In January 2021, following a cyberbullying scandal which dominated headlines, the country of Newtonland passed the Protection Of Children Online Act ("the POCO Act") . The Act contained the following relevant provisions:

Section 1: Scope

(1) This Act aims to protection children against cyberbullying and other forms of harassment in order to protect their safety and mental and physical well-being.
(2) The Act is without prejudice to the Newtonland Privacy Act.

...

Section 2. Definitions

…

(5) "Information society service" shall be defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

(6) "Information society service provider" shall be defined as any party offering or providing internet services.

…

Section 4: Offering of encrypted online communication services to a child

(1) All information society service providers which offer online communication services in such a way that they can be used or accessed by children must ensure that they are able to decrypt such messages if ordered to do so.

(2) Such orders shall be made from the Court of Newtonland on application by the Newtonland Police Force or the Newtonland Child Services. The Court shall only order such decryption if it deems that there is a sufficient risk to the health and mental or physical safety of a child and that the decryption is necessary for the protection of that child. When making such an order, the Court must take due consideration of the right to privacy as enshrined in the Newtonland Privacy Act.

(3) Within 7 days of such an order being made:
(a) Where the encrypted messages are retained by the information society service provider, that provider must send both an encrypted and decrypted version of those messages to the Newtonland Police Force and/or Newtonland Child Services, as appropriate.
(b) Where the encrypted messages are stored on a local device, the information society service provider must transmit any relevant or necessary encryption keys, methods or programs to the Newtonland Police Force and/or Newtonland Child Services, as appropriate.

(4) Where encrypted messages are only stored on a local device, the order may require the owner of that device to allow the Newtonland Police Force or Newtonland Child Services to take a copy of all encrypted messages stored on that device.

(5) This section shall apply whether or not the information society service provider retains copies of such messages. Nothing in this section obliges service providers to retain copies of messages sent.

(6) Failure to enable decryption shall be punishable by a fine of up to €75,000 per message.

…

The Newtonland Privacy Act includes the following provisions.

Section 3: EU Data Protection Law
(1) This Act incorporates and implements Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 into Newtonian law.

(2) This Act incorporates and implements Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 into Newtonian law.

Section 4: Protection of children

(1) Children merit specific protection regarding their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children […] in information society services.

(2) For the sake of Newtonian Data Protection Law, a child shall be considered any person under the age of 13.

The POCO Act had been championed in the Newtonland Parliament by Amos Ivormac, M.P. During a particularly key debate, Ivormac had made the following speech:

“Section 4 of the POCO Act is particularly vital for ensuring that our children do not fall victim to bullying or abuse online. Too often, children are talking to each other—or even to adults!—online and those messages are locked behind encryption. And yet, when we go to the people who peddle these messaging apps, they cry ‘Sorry, we can’t help you! There’s nothing we can do!’

“This encryption means that our police and our child services are totally unable to read what is happening, totally unable to help those children. Without access to these messages, we simply cannot keep our children safe. This provision will mean that our agencies will be able to access those messages if and when it becomes necessary. By mandating that information, society service societies develop and maintain a way to decrypt these messages, we will ensure that we can identify and track down those who might try to do our children harm.

> "For those of you worried about privacy, don't be. Our country has a long history of respecting human rights, which have been enshrined in national law after our adoption of the European Convention of Human Rights. To ensure our utmost compliance with both our national and international obligations, the section has been specifically written such that messages will only be decrypted if an independent judge, looking at all the evidence, deems that the decryption is necessary to protect a child. Furthermore, this provision protects privacy as it ensures that there is no need for mass retention of messages or metadata. My department, which has performed extensive research in the drafting of this law, has discovered that the incriminating messages are retained on both the victim and perpetrator's phones or computers in the vast majority of cases. This is not a question of finding a *copy* of the data, it is a question of being able to *read* that copy—and this Act is specifically designed to address that, and only that, problem."

Bertie, a twelve-year-old child, had received a new phone for his birthday and had initially been very excited. However, after owning the phone for six months, he had complained to a teacher that "I hate my phone; it just gives people another way to bully me." The teacher, who had recently seen Bertie be approached by some boisterous older teenagers on the way home, notified the headmaster. After observing Bertie for a week, the headmaster concluded that Bertie seemed unusually anxious, and so notified the Newtonland Child Services. Based on the information from the school, the Newtonland Child Services applied for an order for the decryption of messages sent and received by Bertie. The order was granted and the Newtonland Child Services used the relevant decryption keys to decrypt and review all of the messages on Bertie's phone. Most of the messages on which were decrypted and reviewed were between Bertie and his family, or between Bertie and other children at his school. The decrypted and reviewed messages also included messages between Bertie and Ms Debussy, the pastor at Bertie's church, although there was no suspicion that Ms. Debussy had been bullying Bertie, or had in any other way acted inappropriately or illegally.

Ms. Debussy brought an action before the Newtonland High Court, alleging that the decryption of the messages had violated her right to privacy under the European Convention on Human Rights, art. 8 and challenging the legality of the Protection of Children Online Act, s. 4.

The Newtonland High Court found that neither the order nor the POCO Act, s.4 violated the ECHR. In its decision, the High Court found that the provision was necessary in a democratic society for the prevention of disorder or crime, for the protection of health or morals, and for the protection of the rights and freedoms of children. In particular, the Court noted that the provision had a relatively narrow scope, had been implemented on the basis of significant research by the Newtonland Parliament, and was subject to judicial oversight. Although it recognised that Ms. Debussy's privacy had been impacted, and there was nothing to suggest that she had done anything wrong, the Court concluded that this was necessary as there was no way to tell which messages were relevant until after they had been decrypted and reviewed.

Ms. Debussy applied to appeal this decision, but this was rejected. Following that rejection, Ms. Debussy lodged an application with the European Court of Human Rights (ECtHR), alleging a violation of her art. 8 rights.

She argued that the POCO Act, s.4 has not been shown to be necessary in a democratic society for the prevention of disorder or crime, for the protection of health or morals, and for the protection of the rights and freedoms of children. In particular:

1. Although the detection, investigation and prevention of cyberbullying is a laudable goal, it is not sufficient to justify the decryption of private and personal messages.
2. Even if decryption might be necessary in some cases, a single order made under that section can cover messages to and from multiple people and there is no way to know who

will be affected before the messages have been decrypted. The section does not contain sufficient controls to protect the rights of those citizens and it is impossible to know whether decrypting some or all of the affected messages is necessary at the time that the order is made.

3. The Act failed to provide proper protections and controls for the protection of privacy after the decryption had taken place. At a minimum, the order should set a scope for which messages can be reviewed once the decryption has been made and require that the Newtonland Police Force or Child Services immediately delete any decrypted messages that are outside of this scope.

Teams must submit two memos, one on behalf of Ms. Debussy as the applicant and one on behalf of Newtonland as the respondent.

Mooters should disregard issues of admissibility and only address the merits of the case. For the purposes of the moot, mooters should disregard pleading requirements and guidelines issued by the ECtHR, and must instead follow the requirements set out in the moot's Rules of Procedure. Submissions must be made before the deadline, as indicated in the moot's timetable.