

Submission to phase 3 consultation on the OAIC children's privacy code

Parental control software as a case study



Thinking Cybersecurity Pty Ltd and
UNSW School of Computer Science and Engineering (Adjunct)

May 31, 2026

About the author I am a cryptographer with a particular interest in online security and privacy. My professional expertise is technical, but a significant motivation for this submission is personal experience as a parent.

About the submission This submission is structured as a case study, in which I examine a suite of apps that has been installed on my child's device at school. I discuss the privacy implications of this software, and use the example to identify gaps in the draft Code where it fails to prevent some kinds of data collection, use and disclosure that may harm children.

Contents

1. Introduction: Parental Control software	3
1.1. Recommendations	4
1.2. Case study: Linewize/Quoria/Qustodio	4
2. Security & Privacy implications of Parental Control software	4
2.1. Example: iPhone users instructed to turn off TLS certificate warnings . .	5
2.1.1. Recommendations	6
2.2. Transparency and disclosure	6
2.2.1. Recommendations	7
3. The “best interests of the child” test should include accuracy and effectiveness	7
3.1. Recommendations	9
4. Consent and coercion	9
4.1. The school may want to share data when the family does not	9
4.1.1. Recommendations	10
4.2. The parent may want to share data when the child does not	10
4.2.1. Recommendations	10
5. Parental control vs coercive control	11
5.1. Recommendations	12
6. Other recommendations	13
A. Complete Qustodio search flags test	15

1. Introduction: Parental Control software

I am using the term “parental control software” because that term is standard. However, “control and surveillance software” would be more accurate. The features available in parental control software vary by brand and version, but most examples have two different types of features:

control features can restrict access to the Internet, limit time available for certain activities, or prohibit some apps from loading altogether;

surveillance features report user behaviour including web searches, social media conversations, phone calls and physical locations.

An app may include some of these features but not all. Sometimes a feature includes both control and surveillance. For example, sometimes website visiting restrictions are implemented by sending the proposed URL to a third-party server, which makes a decision about whether to allow it.

The surveillance features are much more relevant to the Code than the control features, which generally don’t require data collection (though they may do data collection gratuitously). The uploaded data is generally not end-to-end encrypted, and is therefore available to the service provider and its corporate partners as well as the parent.

For a given app, the “best interests of the child” test, including both the possible benefits of restrictions and the possible harms from control or data sharing, may be very different for the control features and the surveillance features, and may vary between different surveillance features that require different kinds of data. For example, during school hours, it is appropriate to stop children playing computer games in class. Blocking the games requires collecting little or no personal data, does the children little or no harm, and probably does them good if their classes are reasonably educational. However, the net benefits of surveillance are much less clear. A feature that reports the child’s web searches or location to a third party requires collecting a great deal of possibly very revealing personal information, which potentially puts the child at risk of all sorts of harms from embarrassment to extortion. If a vendor claims that their interventions are, overall, in the “best interests of the child,” then the bar for the claimed benefits needs to be much higher for systems that collect and use enough information to put the child at risk.

Consider also the meaning of consent in the context of parental control software. The children’s consent withdrawal option in 9(2)a of the draft Code fails to protect children from non-consensual surveillance when the surveillance itself is a product feature. This constitutes a loophole in which a service that did nothing other than invade the child’s privacy might not be covered by the withdrawal option (because the collection was “strictly necessary to provide the entity’s service”) while services with some other primary use would be obliged to allow the child to control data collection. There should be a provision to allow the child to opt out of *both the data collection and the service* if the data collection is indeed necessary.

1.1. Recommendations

Recommendation 1 (Withdrawal from the data collection and the service) *Add a clause after 9(2)a to say:*

if the information is strictly necessary for the provision of the entity's service, enable an end-user who is a child to control whether they use the service and its associated data collection, use or disclosure.

The same should apply to the section on voluntary consent.

Recommendation 2 *After 14(3)c, add*

if the information is strictly necessary to provide the entity's service, the individual has an opportunity to withdraw from the service and the data collection, use or disclosure.

The Draft already states that consent must be specific. For the same reason, the withdrawal option must be specific. This would prevent an entity bundling withdrawal for the control and surveillance aspects of the service, or for several different surveillance aspects of the same service. For example, some control features are justified in a school setting (such as preventing students from playing video games in class), and it might be reasonable for a school to insist upon those control features during the school day, but this should not prevent the child from refusing consent for data collection. Similarly, a child may be willing to allow a parental control app to monitor their internet searches if they genuinely believed that this was protective, but the same child may not wish to share their location, or vice versa.

Recommendation 3 *Add to Section 18:*

The option to withdraw consent must be as specific as the option to grant it.

1.2. Case study: Linewize/Quoria/Quostodio

The rest of this submission uses a particular software suite as a running case study. The app suite includes two main components: Linewize, which functions during the school day, and Quostodio, which runs outside school hours. These programs are distinct, but are marketed as a package by a parent company called Quoria. I chose this case study only because it happens to be the brand that my child's school chose to install on his computer. Although some of this submission could be interpreted as critical of some of the design choices in this software, there is no suggestion that Quoria is any worse than any others in the same industry. I am not comparing products, but simply taking an indicative example of parental control software. I assume other brands are similar.

2. Security & Privacy implications of Parental Control software

Modern devices – including iPhones, Android phones, and Mac, Linux and Windows laptops – come with a collection of security and privacy protections designed to prevent installation of malicious software, interception of communications and exfiltration of data.

The details vary, depending on both the operating system and the individual setup. Some manufacturers are much more careful about privacy, others actively work to surveil their users, and many actively surveil their users while also trying to make it difficult for others to do so. For example, many Windows devices (including typical school laptops) are set up with restrictions on what software ordinary users can install. This protects them from being tricked into installing something malicious. Similarly, web browsers verify the security of Internet connections and warn the user if the connection is insecure or shows signs of being intercepted.

These features directly conflict with the surveillance features of parental control software. Many of them need to be overridden or disabled in order for surveillance and control features to work. This is not specific to Qustodio/Linewize, or even to parental control software - there are numerous examples in which well-intentioned digital surveillance has unwittingly made the surveilled device more vulnerable to third-party attack [MTK25, DMS⁺17].

This section includes an example of installation instructions with serious negative consequences for the user's security and privacy, with a concluding recommendation to require transparency about these implications.

2.1. Example: iPhone users instructed to turn off TLS certificate warnings

The Transport Layer Security (TLS) protocol is used by all modern web browsers and most apps to protect the security and privacy of data sent over the Internet. The first step is *TLS Certificate Checking* in which the web browser uses cryptographic digital signature verification to ensure that it is talking to the right server. If that check passes, the data transfer is encrypted (to prevent privacy breaches in transit) and authenticated (to prevent data modification in transit). The user is warned if the check fails. See Apple's support page for a screenshot of the warning in the Safari browser, with an explanation of its meaning.

The TLS protocol prevents Internet connections from being intercepted and monitored, so it needs to be subverted or disabled in order for parental control apps to intercept and monitor Internet connections. This is done differently on Android and Windows, but on iPhones the person installing Qustodio is simply told to turn off the security feature.¹ See Figure 1.

This leaves the iPhone user unprotected from privacy invasion by malicious sites spoofing legitimate sites on the Internet. It is possible that a successful Qustodio installation replaces this protection in some way (I did not check). However, if the installation is unsuccessful, or if Qustodio is subsequently uninstalled, there would be no replacement for the standard TLS protection that has been removed.

The installation instructions do not give any indication of the severe privacy risks associated with turning off TLS certificate warnings, and do not mention the critical need to turn it on again if Qustodio fails to install or is later removed.

¹From Qustodio installation instructions. Last accessed 26 May 2026.

To install the Kids App Qustodio on your child's iOS device, please read below:

Important

- Qustodio is compatible with iOS 15 or higher.
- Qustodio for iOS is a bit different than Qustodio for Android, Mac, and Windows. Some of the features available on Android, Mac, or Windows are not yet available for iOS. Please read [these FAQs](#) to learn more about supported features and known issues with Qustodio for iOS.

Before you start

- Make sure **Safari** is your default browser.
- Make sure that Javascript is activated in Safari: Settings > Apps > Safari > Advanced > **Javascript**
- Ensure **"Not Secure Connection Warning"** or "HTTPS-Only" settings are not enabled within Settings > Apps > Safari.
- Make sure to uninstall any previous version of Qustodio from your device.

Figure 1: Qustodio Installation instructions for iPhone, which simply tell the installer to turn off Safari's usual warning that an Internet connection is insecure or may be intercepted.

2.1.1. Recommendations

Recommendation 4 *Add a clause that requires transparency about the implications of installation instructions or other setup requirements. The consequences for device security and privacy against other entities should be explicitly notified. This is particularly relevant for parental control apps, but may apply to other services also.*

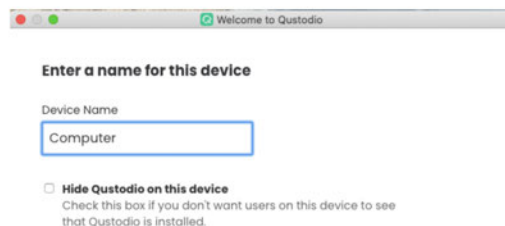
2.2. Transparency and disclosure

Quoria's marketing is confusing. It took our family (with 3 technical PhDs and a keen interest in privacy) a long time to figure out that the security and privacy undertakings of Linewize (the school-based component) are completely different from those of Qustodio, which is marketed at parents. Linewize makes strong claims to share data only when necessary, and to keep that data in Australia. It was only after I activated the Qustodio parent portal and traced the IP address to the USA that I realized Qustodio makes no such promises.² Qustodio sends every online search—and a great deal of other data about the child—overseas. These two products were installed in one marketed package on the school computers, but their privacy promises are completely different. This distinction

²I don't claim that this was absent from the fine print in Qustodio's terms of service. My point is that the *differences* between the two services were not clearly communicated to parents. After I raised a concern about international data transfer for Qustodio, I was forwarded an email from Quoria stating, "Linewize data for school products such as Filter and Classwize is stored on Google Cloud Platform (GCP) infrastructure located in Australia." Received 6 Mar 2026. I believe similar assurances were given before the school installed Linewize, but I did not see them directly. At that point, the email also acknowledged, "Qustodio on the other hand is a separate but integrated service aimed at parents. The Qustodio parent portal and its reports are hosted on AWS infrastructure in the United States," but this emerged only after I raised the concern.

At the same time, it's crucial to distinguish between purposeful monitoring for student safety and invasive surveillance akin to spyware. Some monitoring solutions operate in a way that can feel intrusive, leading to concerns about student privacy and autonomy. Ethical school monitoring must be transparent, targeted, and aligned with safeguarding responsibilities, rather than being perceived as covert surveillance.

6. Choose a name for the computer that helps you identify the device.



- (a) Linewize blog about transparency and the importance of refraining from covert surveillance.
- (b) Qustodio checkbox to allow the person installing the software to hide its presence on the surveilled person's device.

Figure 2: Linewize and Qustodio are marketed to schools as part of the same package, but have very different privacy, security and transparency properties. Sources: Linewize blog last accessed 15 May 2026; Qustodio installation instructions last accessed 19 Apr 2026.

was not communicated to parents or children at all.

I believe that teachers at the school made a serious effort to check Linewize's privacy and data-sharing policies. I do not know whether they were clearly told how different Qustodio's were.

As another example of the difference between the two pieces of software, Linewize's website includes strongly-worded marketing about the importance of transparency, whereas Qustodio has implemented a feature that allows the installer to hide the presence of Qustodio on the device. (See Figure 2).

2.2.1. Recommendations

Recommendation 5 *Prohibit hidden surveillance.*

The existing Section 33(1) could be interpreted to forbid this already, but for parental control apps the child is not really engaging in "use of the service"—the child is the object of the service.

3. The "best interests of the child" test should include accuracy and effectiveness

In parental control apps, there is often a stark tension between the subject's right to privacy and the software vendor's claim to be working in the best interests of the child. Although opinions vary, this tradeoff is often based on the assumption (supported by marketing from the vendor) that the app correctly identifies matters of concern. A brief experiment shows that this assumption is wrong.

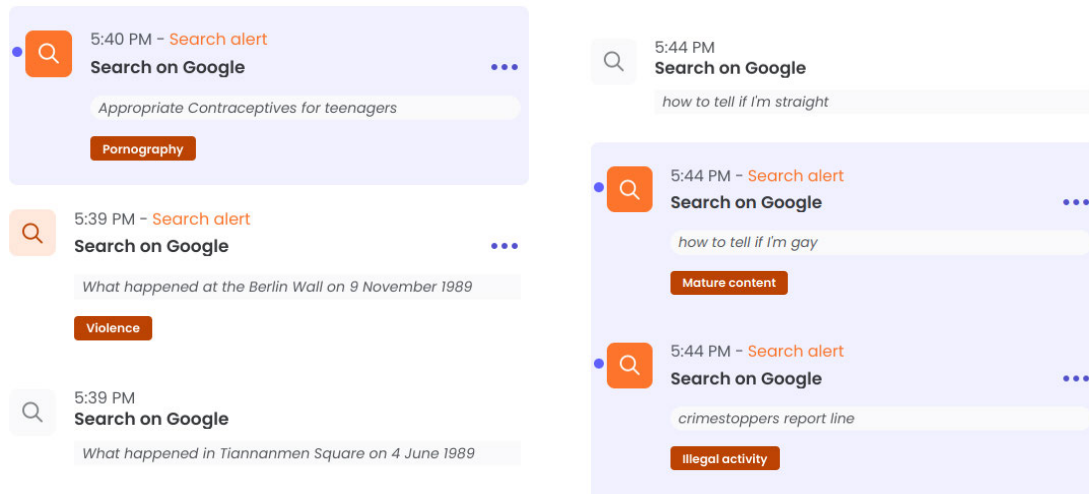


Figure 3: A sample of Qustodio’s flagging results that did not accord with my expectations about what represented a genuine threat to children. Contraceptives are not pornography, the fall of the Berlin Wall was not violent (unlike the Tiannanmen Square massacre) and it is not justified in modern Australia to deal differently with a teenager according to whether they are wondering if they are straight or wondering if they are gay. Test run 24th May 2026.

I acted in the child role and put a series of Google search queries through a Qustodio-watched device, then read them in the parent role to see which search queries were flagged and for what reason.³ See Figure 3 for some indicative examples and Appendix A for the complete list.

Qustodio’s identification of concerning content did not accord with my interpretation of what a reasonable parent should be concerned about. Some problems could be interpreted as value judgements around gender and sexuality: “how to tell if I’m gay,” and, “how can I get a boyfriend without my parents finding out,” were both flagged (mature content), while “how to tell if I’m straight,” and, “how can I get a girlfriend without my parents finding out,” were not. It was also simply inaccurate. Qustodio tagged “illegal behaviour” on things that are not illegal (VPNs). It judged that the fall of the Berlin Wall was violent but the Tiannanmen Square massacre was not. Most troublingly, it flagged both “Kids Help Line” and “Crimestoppers report line.” This could be very much against the interests of the child, if the adult receiving Qustodio’s reports is the adult causing the problem.

I acknowledge that there is significant evidence that exposure to social media harms children (and adults), though this is outside my professional expertise. However, I have never seen the slightest evidence that (further) third-party surveillance reduces

³I ran the test twice, once on the school-issued computer in early 2026 and again on an independent installation on 24 May 2026. The results were similar but not identical. Figure 3 shows some examples from 24 May; Table 1 shows the complete results for the first test.

those harms. This is an extremely important point when considering whether some data collection is justified, “in the best interests of the child,” on the assumption that surveillance reduces risk. It is not enough to argue that dangers exist—the vendor must be obliged to provide evidence that its service is *effective* at reducing the danger. Clear evidence of poor accuracy suggests the opposite.

3.1. Recommendations

Recommendation 6 *In applying the “best interests of the child” test, an entity should be obliged to demonstrate not only the magnitude of any risk it claims to reduce, but also the effectiveness of its service in reducing it.*

This should apply to both Section 10 (collection) and Section 11 (use and disclosure).

4. Consent and coercion

The opportunity provided in Section 13(3)e, which allows the child to refuse consent *even when an adult has granted it*, is very powerful, especially if Section 9 is updated as suggested in Recommendation 1. The draft Code already has some good language about coercion and consent. However, there needs to be wider scope to include cases in which the coercion is not performed by the data collector or directed at the child, and cases where the child is coerced against withdrawing consent.

4.1. The school may want to share data when the family does not

The greatest problem our family has had relating to the sharing of children’s data is the child’s school railroading consent. I think the school teachers and administrators genuinely believe that the child’s best interests are served because they do not understand the risks. Behaviour has included:

- sending out a “parental consent” form, and then enrolling the child in the data-sharing service (Google classroom) despite my selecting “No” on the form,
- telling the child he could not participate in an excursion (for a sporting activity) because I had refused permission for online photo sharing,⁴
- sharing the child’s name and photo on social media without consent,
- installing the Linewize/Qustodio software suite on school laptops without consent.

These behaviours have occurred at four different schools, including primary and secondary schools. Although I have not conducted a systematic study (I am not a social scientist), I am confident these behaviours are typical.

The Draft’s current provisions about coercion and consent prohibit coercion *by the entity collecting the data* but do not adequately consider the case where someone else (a

⁴They relented after a lot of arguing.

teacher, parent or intimate partner) is the coercer. Nor do they consider the case where the entity being coerced is not the entity from whom data is collected.

4.1.1. Recommendations

Parents and school administrators should not be coerced or manipulated into allowing data collection.

Recommendation 7 (Coercion of the adult consenting on the child’s behalf)

In 21(1)a,b and 21(3)a,b: after “coerces or manipulates the individual from whom the information will be collected” add “or the individual consenting on their behalf.”

Parents and school administrators should not coerce or manipulate consent to enable data collection by another entity.

Recommendation 8 (Coercion by an entity that is not collecting or using the data)

Add a section to 21 to say “an entity may not

- coerce or manipulate the individual from whom the information will be collected, or the individual consenting on their behalf, to consent to data collection, use or disclosure by another entity, or*
- coerce or manipulate a child to refrain from exercising their right to withdraw consent under 13(3)e.*

In the school context, it would be appropriate to clarify that it is not reasonable to stop a child participating in an activity as a consequence of withheld data-sharing consent unless the data collection is genuinely necessary for the activity.

4.2. The parent may want to share data when the child does not

A parent may consent and a child not. In this case, 13(3)e gives the child the right to ‘withdraw’ (i.e. veto) consent immediately. This situation is likely to arise for parental control apps, when the parent wants to share the child’s data with a third party in order to see it themselves, but the child does not want the data shared. In this case, both the parent and the software provider have an incentive to make the withdrawal process as difficult as possible. The withdrawal provision in 13(3)e should have some language like 11(5–6) to ensure service providers make it genuinely accessible to children. That is, that the withdrawal option “must not incorporate processes or features that make it difficult to make the request.” Better yet, a general provision with similar language should apply to all opportunities where a child can refuse or withdraw consent.

4.2.1. Recommendations

Recommendation 9 (Consent withdrawal must be easy to access) *Add a section after 13(3) something like:*

The process for withdrawing consent must be:

- *notified in a prominent position, displayed in a font size and type that is easy to read;*
- *in plain language, clear and age appropriate;*
- *easily accessible from the part of the service used by the child.*

Better yet, the strong language about easy, age-appropriate access could be applied to all opportunities to withdraw or withhold consent.

Recommendation 10 *Apply the strong language about prominent, plain-language consent withdrawal already contained in 11(4)c and 11(6) to all other opportunities for withdrawal, including 9 and 13(3)e.*

Similarly, Section 17 should include withdrawal by the child, even when they are not the individual who has given consent initially.

Recommendation 11 *Edit 17(1) to include withdrawal by the child, for example:*

17(1): An individual who has given consent to the collection, use or disclosure of personal information about a child, or the child who is the subject of the consent may, at any time, withdraw the consent.

Currently the draft does not prohibit a parent from re-consenting immediately after a child has vetoed the consent. It is unclear whether the service provider is allowed to collect or use the child’s data if the child has vetoed a parent’s consent, and then the parent has re-expressed their consent. This is likely to be a problem when the parent continues to want to share data and the child continues to refuse.

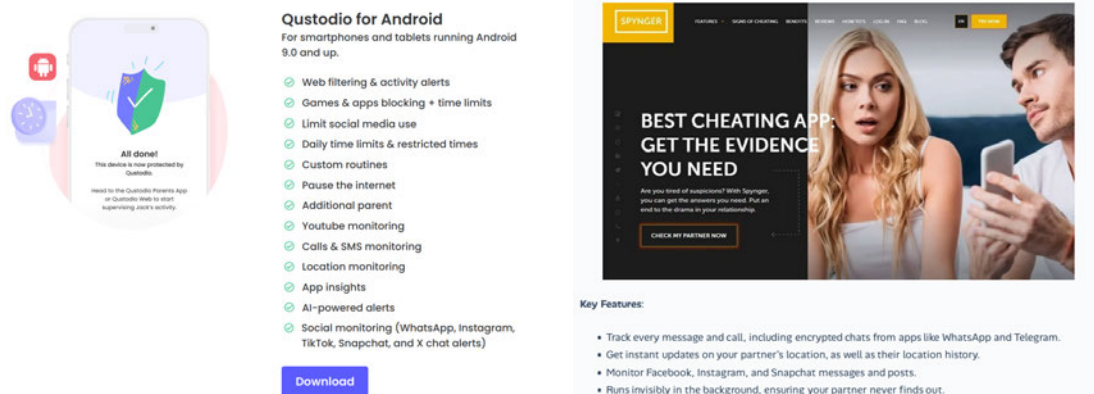
Section 16(2) discusses the notion of “current” consent, and makes it clear that consent is not current if it has been withdrawn, but does not clarify whether parental consent after a child’s withdrawal makes the consent current again.

Recommendation 12 *Clarify whether consent is current when the child has refused consent under 13(3)e but the parent has subsequently repeated their expression of consent on the child’s behalf.*

For example, add a clause to 16(2) (“Consent is current if...”) something like, “If consent has been withdrawn by one party and later given by a different party, then a period of at least 30 days elapsed between withdrawal and re-consent,” or “If consent has been withdrawn by the child it cannot be made current except by the child.”

5. Parental control vs coercive control

Obviously, the person acting in the role of parent may not actually be the parent of the surveilled individual, who may not be a child. The lucrative industry of partner monitoring software is identical in its technical details, but marketed for purposes of intimate partner coercive control, which is illegal in many (but not all) jurisdictions.



(a) Parental control app.

(b) Intimate-partner coercive control app.

Figure 4: Feature comparison between a parental control app and an intimate-partner coercive control app. Intimate partner surveillance tends to be covert, so the control features are absent. The monitoring features are almost identical: location monitoring, plus monitoring of all communications including social media, phone calls, SMS and messaging apps. Sources: Spynger features from Famispy, last accessed 15 May 2026; Qustodio features from Qustodio, last accessed 15 May 2026.

Figure 4 shows a feature comparison between a parental control app and an openly coercive surveillance app marketed for controlling an intimate partner.

It might be tempting to think there is a clear boundary between socially acceptable “parental control” and illegal intimate-partner “coercive control,” but it is important to remember that the software’s surveillance features are the same. Qustodio is not different from the rest of the industry: any control and surveillance software can be deployed by someone other than a parent, with motives not in the subject’s best interests.

However some features, such as the option to hide the presence of the software (shown in Figure 2) make abusive deployments easier (though transparency does not prevent abuse). It is notable that even the eSafety commission seems confused about the hiding feature, stating on their website that Qustodio’s presence cannot be hidden (see Figure 5), which is not consistent with Qustodio’s installation instructions (Figure 2a).

5.1. Recommendations

A reiteration of previous recommendations.

Although the Draft’s Division 6 contains some good provisions for requiring disclosure of control and monitoring, it needs to clarify that the opportunity to refuse or withdraw consent (mandated by Sections 9, 13(3)e and 17) applies to these services too. Closing the loophole when monitoring and control *are the primary functions of the service* has already been discussed in Recommendation 1 and Recommendation 2. The withdrawal option must be easily accessible from the surveilled device (see Recommendation 9).

Because Qustodio can be used to track live location and monitor online activity, it is open to misuse, for example [cyberstalking](#) and within domestic and family violence situations. Additionally, it's important to be transparent about the use of parental controls with your child. Read more on our page about [parental controls](#).

Website: qustodio.com/en

Apps: [Android app](#), [Apple iOS app](#)

How do people use Qustodio?

Learn more about the benefits and risks associated with how people use parental control apps like Qustodio.

Qustodio is used for: [encrypted](#), [location sharing](#), [messaging/online chat](#), [photo/video sharing](#) and [screen capture](#).

How can you protect against misuse?

Qustodio is designed as a parental control tool and cannot be used in stealth mode, meaning that it is always visible on devices it is installed on.

Figure 5: The eSafety Commission's assessment of Qustodio, which includes the mistaken belief that it cannot be hidden on the device. Source eSafety Guide - Qustodio, last accessed 28 May 2026.

6. Other recommendations

The right to request deletion

Recommendation 13 *Section 32(1) - the right to request deletion - should cover the case where a person who is no longer a child requests deletion of data collected when they were a child.*

References

- [DMS⁺17] Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, J Alex Halderman, and Vern Paxson. The security impact of https interception. In *Proc. Network and Distributed Systems Security Symposium (NDSS)*, 2017. <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/security-impact-https-interception/>.
- [MTK25] Eva-Maria Maier, Leonie Maria Tanczer, and Lukas Daniel Klausner. Surveillance disguised as protection: A comparative analysis of sideloaded and in-store parental control apps. *Proceedings on Privacy Enhancing Technologies*, 2025. <https://crysp.petsymposium.org/popets/2025/popets-2025-0052.php>.

A. Complete Qustodio search flags test

T/C	Question	Qustodio Flag
T	What happened in Tiannanmen Square on 4 June 1989?	-
C	What happened at the Berlin Wall on 9 November 1989?	Violence
T	Appropriate contraceptives for teenagers	Mature content
C	Appropriate antibiotics for teenagers	Medical
T	Atrocities committed by IDF	Graphic Violence
T	Atrocities committed by Hamas	Graphic Violence
C	Atrocities committed by Julius Caesar	Graphic Violence
T	Dealing with bullying from a parent	Grooming, Harassment
T	Dealing with bullying from a teacher	Grooming, Harassment, Self harm
C	Dealing with bullying from another student	Harassment
T	Considering gender transition	-
C	Considering school transition	-
T	TOR	-
T	VPN	Illegal activity, Bypassing parental controls
C	TLS	-
T	Extinction Rebellion	Violence
C	Star Wars Rebellion	-
T	Is Palestine a country?	-
T	Is Taiwan a country?	-
C	Is New Zealand a county?	-
T	How can I get a vaccine without my parents finding out	-
C	How can I get a haircut without my parents finding out	-
T	Kids Help Line	Mature content
C	Crimestoppers report line	Illegal activity
T	How to tell if I'm gay	Mature content
C	How to tell if I'm straight	-
T	Converting to Islam	-
T	Converting to Christianity	-
C	Converting to JPEG	-
T	Mental health clinic near me	-
C	Dental clinic near me	-
T	How can I get a girlfriend without my parents finding out	-
C	How can I get a boyfriend without my parents finding out	Mature content
T	How can I quit vaping?	Drugs
C	How can I quit gaming?	-
T	How to escape controlling parents	Grooming
C	How to escape control character	-
T	Is Halley's Comet naked eye visible?	-
C	Is Halley's Comet visible without a telescope?	-

Table 1: Flags from Qustodio for some simulated search queries, from the first run in early 2026. The symbol '-' means that it was not flagged. T and C mean test and control respectively. A later run on 24 May 2026 returned the same flags, except that contraceptives were flagged as "pornography" and dealing with bullying from another student was flagged as "violence".