Submission to the Office of the Australian Information Commissioner

Response to the Exposure Draft

Privacy (Children's Online Privacy) Code 2026

Focus issue: monitoring, control and surveillance of children

Submitted to: Office of the Australian Information Commissioner
Document: Response to the OAIC Child Privacy Code exposure draft
[redacted]
Professional background: Cybersecurity and privacy
Date: June 5, 2026

Cover Letter

Office of the Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Dear Commissioner,

Thank you for the opportunity to comment on the exposure draft of the *Privacy (Children's Online Privacy) Code 2026*.

I make this submission in my personal capacity. I work in cybersecurity and privacy, including the assessment of digital services used by children and young people across privacy, security and online safety risks.

I am supportive of the proposed Code and the OAIC's approach. The draft Code appropriately recognises that children are not merely passive users of digital services, but rights-holders whose privacy, autonomy, development and participation should be protected. I particularly support the Code's focus on strict necessity (which aligns internationally), the best interests of the child, meaningful access rights, deletion rights, complaints processes and privacy impact assessments.

My submission focuses on three connected issues I have observed in digital services used by children and young people:

1. **Monitoring, control and surveillance:** Division 6 should treat scanning, profiling, geolocation tracking, screen viewing, communications monitoring and automated risk scoring as substantive interferences with privacy, not merely features requiring notice.
2. **Developmental and psychological harm:** Privacy is part of healthy development. Overbroad monitoring can chill expression, reduce trust and help-seeking, and undermine autonomy, self-regulation and participation. Surveillance or monitoring has also been proven to result in psycological changes in developing children that must be considered.
3. **Commercial incentives and design risk:** Safety, welfare and parental-control language should not allow providers to normalise intrusive data collection, build behavioural intelligence from children, or monetise control-oriented products without strict necessity, proportionality and child-rights safeguards.

In my work assessing services used by children and young people, I have seen a wide spectrum of privacy risk. Some services involve limited handling of information. Others are designed around persistent observation, behavioural control or automated escalation, including scanning, tracking, recording, flagging, scoring, profiling, geolocation monitoring, live screen viewing, communications monitoring and inferred wellbeing or risk assessments. These systems are often advertised as safety, care or convenience, but can interfere significantly with children's privacy, autonomy, expression, help-seeking behaviour and development.

These risks are not hypothetical. The NSW Crime Commission's *Project Hakea* report found that tracking and other surveillance devices are frequently used to stalk, harass, intimidate and monitor victims of domestic and family violence, and can facilitate serious criminal harm (New South Wales Crime Commission 2024). While that report concerned criminal misuse of tracking and surveillance devices, it demonstrates why monitoring capabilities should not be treated as benign merely because they are presented as safety, care, welfare or parental-control features. In the context of children's online privacy, the Code should recognise that monitoring can itself

be a serious interference with privacy, autonomy and development.

My central recommendation is that the Code should treat monitoring and control mechanisms as substantive interferences with children's privacy, not merely as features requiring notification. Notification is important, but it is not sufficient. Where a service enables tracking, scanning, recording, profiling, flagging, scoring or otherwise observing a child's activity, communications, location, device use, behaviour or inferred wellbeing, that functionality should be assessed against legality, necessity, proportionality, the best interests of the child and the availability of less intrusive alternatives.

The Code should clearly distinguish protective, targeted and lawful safeguarding measures from generalised or continuous surveillance. Children should not be subject to covert, excessive or open-ended monitoring merely because a product is marketed as a safety tool, parental-control feature, education technology service or welfare mechanism. Nor should unparticularised safety, welfare or parental-control claims be sufficient to justify broad monitoring of children's communications, searches, documents, photographs, location, device activity or online behaviour.

I recommend that Division 6 be strengthened so that monitoring or control mechanisms are permitted only where there is a clear lawful basis, a defined child-protective purpose, demonstrable necessity and proportionality, and no reasonably available less intrusive alternative. Where such mechanisms are used, they should be transparent to the child in an age-appropriate way and subject to meaningful safeguards, including data minimisation, security controls, retention limits, human review, limits on disclosure and escalation, access and deletion rights, complaint pathways, and periodic review.

This approach would better align Division 6 with the broader structure of the draft Code, including the requirements that children's personal information be handled only where strictly necessary, consistently with the best interests of the child, and subject to privacy impact assessment where new or changed handling of children's personal information is likely to have a significant privacy impact.

I hope the OAIC will consider the amendments and recommendations set out in this submission.

Yours sincerely,

1 Division 6: Monitoring and control mechanisms

1.1 Core position

The central issue is that monitoring is a substantive interference with children's rights, not merely a feature requiring notification.

The current drafting is useful but too narrow. It focuses mainly on parental control mechanisms and geolocation monitoring. Those are important examples, but they do not capture the broader surveillance capabilities now built into many child-facing, education, wellbeing and safety products.

The relevant practices include monitoring of messages, emails, documents, search terms, browsing history, screenshots, app usage, location data, webcam or microphone access, behavioural analytics, automated content scanning, wellbeing alerts, profiling, risk scoring, keystroke logging and other activity tracking. These practices may be described as safety, wellbeing, parental oversight or educational tools, but they can still involve persistent observation of a child's private life, communications, relationships, identity exploration and help-seeking behaviour.

Recent enforcement action against spyware and stalkerware vendors illustrates why functionality matters more than marketing labels. Products promoted for safety, parental monitoring or oversight can enable covert monitoring of communications, location, calls, messages and device activity. Similar capabilities may appear in child monitoring products. A product marketed as parental monitoring may therefore operate, in substance, as surveillance software.

Australian surveillance law supports the same caution. Monitoring technologies are not regulated only through privacy law. State and Territory surveillance devices legislation recognises that recording, tracking and data monitoring can intrude on privacy, facilitate control and cause serious harm. The NSW Crime Commission's *Project Hakea* report is a useful example because it documents the dual-use nature of tracking and surveillance tools, including products marketed under child or parental safety language (New South Wales Crime Commission 2024). As this report addresses *Project Hakea* elsewhere, Division 6 need only note here that its findings support a precautionary approach to surveillance capabilities marketed as child safety tools.

Notice alone is not enough. A child being told that they are being constantly watched does not make the watching lawful, proportionate, developmentally appropriate or consistent with the child's best interests. Transparency is a minimum safeguard, not the legal basis for monitoring.

A precautionary approach is therefore necessary for covert, continuous, generalised or excessive monitoring of children. Monitoring raises the highest risk where it lacks a clear legal basis, is not directed to a specific and serious child-protective purpose, is continuous by default, or could be replaced by a less intrusive alternative.

Commercial repurposing is a further risk. This is particularly important in school and captive-user contexts, where children may have little practical ability to refuse surveillance or challenge how information about them is used.

Privacy should not be framed as being in conflict with child safety. Privacy is part of child safety. Children need private space to think, communicate, seek support, explore identity, develop judgment, build trust and learn self-regulation. Continuous monitoring may reduce some visible risks while creating deeper developmental, relational and safety harms.

1.2 Recommendations

1. Treat monitoring as substantive interference, not a notification issue.
2. Presume against covert, continuous, generalised or excessive monitoring.
3. Permit monitoring only with a lawful basis, defined protective purpose, necessity, proportionality and strict time limit.
4. Cover message scanning, search tracking, keystroke logging, automated content analysis and AI-enabled monitoring with broad definitions that encompass both current technology and emerging or future surveillance methodologies;
5. Require entities to assess less intrusive alternatives, including digital literacy, trust based evidence proven methods, and safety by design requiring the systems young people use themselves be safe by design in not providing features in the first place that are dangerous and risky to individuals.
6. Require assessment against surveillance, interception and similar laws before monitoring tools are enabled for children and require documentation of any mechanisms or instruments relied on to establish a lawful basis, and document and provide clear and explicit methods to young people to challenge and revoke;
7. Prohibit use of child monitoring data for behavioural profiling, product optimisation, market analytics or machine-learning training and any other commercial uses including internal product analysis and benefits;
8. Any test of the "best interests of the child" must reflect the framework of UNCRC General Comment No. 14, which emphasizes that the best interests concept is "aimed at ensuring the full and effective enjoyment of all rights recognized in the Convention," meaning that no individual right can be used to override or weaken others.
9. The deployment of any monitoring or surveillance tools and services must be governed by the same standards applicable to adults: they must be prohibited by default, authorized exclusively by explicit statutory law, subject to strict transparency obligations, and contingent upon judicial review with ability to challenge or appeal.

Suggested drafting amendment: Division 6 should provide that an entity must not provide or enable a mechanism to monitor, control, scan, analyse, profile, flag, score, record or disclose information about a child's activity, communications, location, device use, behaviour or inferred wellbeing unless the monitoring is authorised by law or supported by a clear legal basis, strictly necessary for a defined child-protective purpose, proportionate, the least intrusive option reasonably available, transparent to the child, time-limited, independently assessed, not repurposed for commercial analytics, disciplinary management, behavioural profiling or machine-learning training, and consistent with the best interests of the child.

2 Health and Wellbeing Services: Commercial Wellness and AI

The Code must protect children seeking health and wellbeing support in digital environments. It should not allow commercial wellbeing, fitness, mood-tracking, mental health, AI conversational or student wellbeing platforms to evade the Code by labelling themselves as "health-related" services.

This distinction is legally and clinically important. The draft Code contains a necessary safeguard for children under 15 who seek legal or health-related support in sensitive circumstances, particularly where a parent, guardian or household member may be implicated in harm or distress. Children must have confidential access to support without interference from commercial data collection.

This safeguard should not create a structural loophole for commercial exploitation. A child accessing emergency support is not equivalent to a commercial platform collecting, profiling, scoring or monetising children's health, mood, sleep, diet or emotional data. Under the *Privacy Act 1988* (Cth) and the Australian Privacy Principles, health information is treated as sensitive information with higher protective standards because of its potential to cause serious harm if misused. Commercial apps that collect health or psychological data must meet strict requirements for consent, necessity, data minimisation, security and confidentiality (Office of the Australian Information Commissioner 2025). Broadly defined health service exemptions should not override these foundational protections.

Empirical research on mobile health and mental health apps confirms significant privacy and security risks in practice. A cross-sectional study of over 20,000 health-related mobile applications found extensive data collection, third-party sharing and inconsistent adherence to privacy norms, raising concerns about user profiling and data misuse (Tangari et al. 2021). Independent empirical analysis of mental health apps revealed security flaws, unnecessary permissions and third-party data transmission that amplify privacy threats for vulnerable users (Iwaya et al. 2023). A critical content analysis of mental health apps also found that many popular apps lacked accessible or comprehensive privacy policies, with a substantial proportion requesting access to device data without clear justification or user benefit (Parker et al. 2019).

These findings are consistent with broader analyses of the digital health landscape. Reviews of mHealth wearables and smartphone health-tracking tools identify trends toward re-identification risks, opaque data flows and inadequate regulatory oversight, underscoring the need for stronger privacy standards aligned with health law and clinical best practice (Suver and Kuwana 2021).

The legal and ethical context for protecting health data is well established. Health privacy law recognises the heightened sensitivity of health information, requiring explicit consent, limited use and robust protections against unauthorised access. International standards, including the *Convention on the Rights of the Child*, further obligate states to ensure privacy and confidentiality for children in relation to their health and personal information (United Nations 1989). By contrast, commercial digital platforms often operate outside medical regulatory frameworks and may not be subject to clinical duties of care or professional confidentiality, creating gaps in legal accountability.

AI and machine learning tools marketed for wellbeing or mental health present similar privacy challenges. Research on direct-to-consumer AI/ML health apps has highlighted that conventional health privacy protections, such as health-specific privacy laws, often do not apply to these commercial tools, exposing sensitive data to broader and less regulated usage con-

texts. These tools can collect detailed behavioural and emotional data, yet standard clinical privacy safeguards, including secure storage and appropriate access controls, are frequently absent (Gerke and Rezaeikhonakdar 2022). Emerging academic work also emphasises the risk that conversational AI systems can lead to over-disclosure of personal information due to misplaced trust and lack of clear boundaries around data collection and reuse, compounding privacy concerns (Anvari and Wehbe 2025).

Given this evidence, foundational privacy protections in health and wellbeing contexts must apply fully under the Code. Exemptions that permit commercial entities to process children's personal data for profiling, targeted engagement, behavioural analytics, direct marketing, secondary use, AI training or non-clinical optimisation would undermine legal and medical standards for confidentiality and harm prevention.

To address these issues, the Code should:

1. **Narrow the health exemption:** Only services provided under direct clinical supervision and meeting statutory medical device or clinical service registration criteria should be considered health services for exemption purposes. Commercial apps that collect health, emotional or behavioural data should be fully bound by the Code.
2. **Tie exemptions to recognised regulation:** Restrict exemptions to software or services that are registered under recognised medical regulatory frameworks and are subject to professional confidentiality obligations.
3. **Prohibit secondary exploitation:** Forbid processing, profiling, targeting or monetisation of children's health-related data for marketing, analytics, engagement optimisation, AI training or any purpose beyond direct clinical care.
4. **Mandate privacy and clinical safeguards:** Non-exempt services should be required to conduct privacy impact assessments, provide age-appropriate and clear disclosure of data practices, implement encryption and data minimisation by design, ensure human clinician review for high-risk assessments, and apply strict data retention and deletion policies.

Children should be able to access genuine clinical care without being treated as data sources for commercial platforms that collect sensitive personal information under the language of care. Fundamental privacy protections in health and wellbeing services are essential, legally mandated and supported by peer-reviewed evidence of risk.

3 General Comments

The following comments set out additional general observations that apply across multiple areas of the draft Code and should be considered alongside the specific recommendations above.

3.1 Ensuring EdTech Is Not Exempted

Educational technology used in schools should not be exempt from the OAIC Children's Online Privacy Code.

Students in compulsory education rarely have a meaningful ability to refuse participation in school-approved digital systems. This makes consent an unreliable basis for collecting, using, or disclosing children's personal information in schools.

Case Study: Facial Recognition in Swedish Schools This issue was tested in Sweden, where Skellefteå High School used facial recognition to record student attendance. The Swedish Data Protection Authority fined the school board SEK 200,000, finding that consent could not serve as the lawful basis for processing because students were in a position of dependency (Integritetsskyddsmyndigheten 2019).

The Authority highlighted the strict requirements for valid consent, noting that:

> 'Consent' of the data subject is defined in Article 4.11 of the General Data Protection Regulation as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Applying this definition to the power dynamics inherent in an educational institution, the Authority elaborated:

> *The scope for voluntary consent within the public sphere is therefore limited. As regards the school sector, it is clear that the students are in a position of dependence with respect to the school both as regards grades, student grants and loans and education, and therefore also as regards the scope to obtain employment in the future or to continue further education. The processing also often involves children's personal data.*

The Administrative Court of Appeal in Stockholm subsequently confirmed the ruling, holding that consent was not freely given and could not justify processing sensitive biometric data under the GDPR (MLex 2021).

The GDPR Framework and Broader Implications The European approach to systemic power differentials is explicitly codified in the GDPR. As Recital 43 states:

> *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*

This European precedent illustrates how structural power imbalances prevent valid consent in education, which is a vulnerability that translates directly to other jurisdictions. In Australia, for instance, students are generally required by law to attend school, and institutions hold substantial authority over them. Consequently, consent is unlikely to be voluntary where access to education, classroom participation, or ordinary school administration depends on using the technology.

That concern is stronger where EdTech systems enable monitoring, communications scanning, automated flagging or behavioural profiling. In those circumstances, vendors should not be able to rely on formal consent forms, school policies, standard platform terms or administrative convenience as a lawful justification for invasive data handling. The relevant question should be whether there is an independent lawful basis, strict necessity, proportionality and a less intrusive alternative, not whether a school has procured or approved the product.

The OAIC should maintain its position that education should not be exempt from the Children's Online Privacy Code. Privacy-invasive educational technology must demonstrate a lawful basis, necessity, proportionality, transparency, and appropriate safeguards. Formal consent, school policy, or administrative convenience alone is insufficient.

The Code should therefore require more than formal consent: it should require necessity, proportionality, data minimisation, transparency, and child-rights safeguards.

This is particularly important where EdTech systems collect sensitive information or enable monitoring. School canteens, classroom tools, learning platforms, device-management software and wellbeing systems may be presented as administrative or safety measures, but they can still interfere with privacy, autonomy and development. Less intrusive options, such as cards, badges, barcodes or local authentication, should be preferred where they achieve the same purpose without collecting biometric or behavioural data.

Monitoring tools also create developmental and psychological risks. AI-driven or continuous monitoring can chill students' expression, reduce trust in adults, and deter help-seeking on sensitive issues such as mental health, sexuality, bullying, abuse, or family violence. Research and civil society reporting on student activity monitoring indicate that these systems can affect search behaviour, self-expression, and disclosure, with heightened risks for marginalised students (Center for Democracy & Technology 2022; O'Daffer, Liu and Bloss 2025).

School-based AI and EdTech systems can also operate with limited transparency and weak oversight. Automated flagging, risk scoring, and escalation systems may generate false positives, embed bias, or extend surveillance beyond school hours and into students' homes. These risks are not resolved merely by notifying students or parents that monitoring occurs.

The OAIC should make clear that EdTech providers must comply with the Code unless a narrow and clearly justified exception applies. Safety, welfare, administrative efficiency or parental-control claims should not be enough to justify broad collection, profiling or monitoring of children. EdTech systems should be assessed against strict necessity, proportionality, the best interests of the child, and the availability of less intrusive alternatives.

In short, educational benefit should not become a pathway for surveillance or commercial exploitation. Children should be treated as rights-holders in educational technology contexts, not as captive data sources.

4 Conclusion

The Code, in my view, has a strong foundation and includes thinking across human rights and other areas that are fundamental to the wellbeing and rights of young Australians.

The Code should continue to be developed and deepened in specific areas. I believe this will be supported through industry and community engagement, and the OAIC's approach to ensuring community engagement, particularly from parents and young people, is critical.

Privacy is a baseline condition for children's safety, autonomy, dignity, and development. Research indicates that overbroad digital monitoring chills expression, reduces trust, and deters children from seeking help on critical health and safety issues.

Treating tracking, content scanning, and behavioural profiling as ordinary product features legitimises the very harms the Code is intended to prevent. The best interests of the child require structural protections rather than disclosure and consent formalities.

The available evidence demonstrates that monitoring capabilities create significant privacy and psychological risks across both commercial applications and educational environments. For example, the Swedish Data Protection Authority established that students exist in a position of dependence, meaning formal consent cannot justify invasive digital processing in schools. Furthermore, reports from the New South Wales Crime Commission and the Center for Democracy & Technology show that monitoring tools are frequently repurposed for intrusive observation or discipline, rather than targeted safety.

The final Code must give practical effect to children's rights by establishing a presumption against covert, continuous, or generalised surveillance. The OAIC should strengthen the draft Code to ensure that safety is achieved through privacy-preserving, rights-consistent design. Children must not be required to surrender their privacy to learn, communicate, or participate in modern digital life.

5 References

American Academy of Pediatrics 2025, *Balancing online safety and independence: Parental monitoring by age*, AAP Center of Excellence on Social Media and Youth Mental Health, Itasca.

Anvari, SS & Wehbe, RR 2025, *Therapeutic AI and the hidden risks of over-disclosure: an embedded AI-literacy framework for mental health privacy*, arXiv preprint.

Burke, C, Triplett, C, Rubanovich, CK, Karnaze, MM & Bloss, CS 2024, 'Attitudes toward school-based surveillance of adolescents' social media activity: convergent parallel mixed methods survey', *JMIR Formative Research*, vol. 8, e46746, doi:10.2196/46746.

Center for Democracy & Technology 2022, *Hidden harms: the misleading promise of monitoring students online*, Center for Democracy & Technology, Washington, DC.

Commonwealth of Australia 1979, *Telecommunications (Interception and Access) Act 1979 (Cth)*, Commonwealth of Australia, Canberra.

Federal Trade Commission 2019, 'FTC takes action against stalking apps', *Business Blog*, Federal Trade Commission, Washington, DC, 22 October.

Federal Trade Commission 2021, 'FTC bans SpyFone and CEO from surveillance business and orders company to delete all secretly stolen data', Federal Trade Commission, Washington, DC, 1 September.

Ford, CA, Millstein, SG, Halpern-Felsher, BL & Irwin, CE 1997, 'Influence of physician confidentiality assurances on adolescents' willingness to disclose information and seek future health care: a randomized controlled trial', *JAMA*, vol. 278, no. 12, pp. 1029–1034.

Ghosh, AK, Badillo-Urquiola, K, Guha, S, LaViola, JJ Jr & Wisniewski, PJ 2018, 'Safety vs. surveillance: what children have to say about mobile apps for parental control', in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, paper 124.

Gerke, S & Rezaeikhonakdar, D 2022, 'Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps', *Intelligence-Based Medicine*, vol. 6, article 100061.

Integritetsskyddsmyndigheten 2019, 'Facial recognition in school renders Sweden's first GDPR fine', Integritetsskyddsmyndigheten, Stockholm, 21 August, updated 6 May 2021.

Iwaya, LH, Babar, MA, Rashid, A & Wijayarathna, C 2023, 'On the privacy of mental health apps: an empirical investigation and its implications for app development', *Empirical Software Engineering*, vol. 28, no. 1, article 2.

Laird, RD, Zeringue, MM & Lambert, ES 2018, 'Negative reactions to monitoring: do they undermine the ability of monitoring to protect adolescents?', *Journal of Adolescence*, vol. 63, pp. 75–84.

MLex 2021, 'Facial recognition usage by Swedish school: judges uphold regulator's decision', *MLex*, 24 June.

New South Wales 2007, *Surveillance Devices Act 2007 (NSW)*, New South Wales Government, Sydney.

New South Wales Crime Commission 2024, *Project Hakea: Criminal use of tracking and other surveillance devices in NSW*, New South Wales Crime Commission, Sydney.

Office of the Australian Information Commissioner 2025, *Guide to health privacy: introduction and key concepts*, OAIC, Canberra.

Office of the Australian Information Commissioner 2026, *Exposure Draft: Privacy (Children's Online Privacy) Code 2026*, OAIC, Canberra.

O'Daffer, A, Liu, W & Bloss, CS 2025, 'School-based online surveillance of youth: systematic search and content analysis of surveillance company websites', *Journal of Medical Internet Research*, vol. 27, e71998.

Parker, L, Halter, V, Karliychuk, T & Grundy, Q 2019, 'How private is your mental health app data? An empirical study of mental health app privacy policies and practices', *International Journal of Law and Psychiatry*, vol. 64, pp. 198–204.

Ryan, RM & Deci, EL 2000, 'Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being', *American Psychologist*, vol. 55, no. 1, pp. 68–78.

Stattin, H & Kerr, M 2000, 'Parental monitoring: a reinterpretation', *Child Development*, vol. 71, no. 4, pp. 1072–1085.

Suver, C & Kuwana, E 2021, 'mHealth wearables and smartphone health tracking apps: a changing privacy landscape', *Information Services & Use*, vol. 41, nos. 1–2, pp. 71–79.

Tangari, G, Ikram, M, Ijaz, K, Kaafar, MA & Berkovsky, S 2021, 'Mobile health and privacy: cross sectional study', *BMJ*, vol. 373, n1248.

UN Committee on the Rights of the Child 2013, *General comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration, Article 3, paragraph 1*, CRC/C/GC/14, United Nations, Geneva.

UN Committee on the Rights of the Child 2021, *General comment No. 25 on children's rights in relation to the digital environment*, CRC/C/GC/25, United Nations, Geneva.

United Nations 1989, *Convention on the Rights of the Child*, United Nations, New York.

Volosevici, D 2025, 'Surveillance as a socio-technical system: behavioral impacts and self-regulation in monitored environments', *Systems*, vol. 13, no. 7, article 614, doi:10.3390/systems13070614.

Whittaker, Z 2022, 'Support King, banned by FTC, linked to new phone spying operation', *TechCrunch*, 17 December.

Wisniewski, P, Ghosh, AK, Xu, H, Rosson, MB & Carroll, JM 2017, 'Parental control vs. teen self-regulation: is there a middle ground for mobile online safety?', in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Association for Computing Machinery, New York, pp. 51–69.