

POLICY AND PRACTICE

A safe glimpse within the “black box”? Ethical and legal principles when assessing digital marketing of food and drink to children

Mimi Tatlow-Golden¹, Valerie Verdoodt², John Oates¹, Jo Jewell³, João J Breda³ and Emma Boyland⁴

¹ The Open University, United Kingdom

² KU Leuven, Belgium

³ WHO Regional Office for Europe, Denmark

⁴ University of Liverpool, United Kingdom

Corresponding author: Mimi Tatlow-Golden (email: mimi.tatlow-golden@open.ac.uk)

ABSTRACT

Marketing in digital media presents major new challenges to those seeking to identify, for research or monitoring purposes, the extent and nature of children's exposure to marketing of foods and non-alcoholic beverages high in fat, salt and sugar. The WHO Commission on Ending Childhood Obesity called for reductions in children's (including adolescents') exposure to such marketing in all media and for the closing of regulatory loopholes. Assessing the extent and nature of such exposure and the effectiveness of proposed regulation is challenging in a new digital media era, however, as marketing is increasingly personalized, based on Internet users' behavioural patterns. The ethics and legality of accessing personal data are not yet clearly established and the closed, “black box” nature of much digital data presents a significant challenge.¹

This paper builds on conclusions of a workshop at the WHO Regional Office for Europe that aimed to inform policy-makers, funders, researchers and regulators by summarizing the ethical and legal considerations researchers need to address in study design. The workshop considered digital ethics guidance, European Union law and terms and conditions of social media platforms; it concluded that such research can be carried out ethically, although it is particularly important for stakeholders to make case-by-case assessments and to view consent as a process. Nevertheless, the terms and conditions of digital platforms and applications present legal access challenges.

Keywords: DIGITAL MEDIA, ETHICS, LAW, MARKETING, ADVERTISING, RESEARCH, CHILDREN, ADOLESCENTS, SOCIAL MEDIA, FOOD

BACKGROUND

WHO's Commission on Ending Childhood Obesity (1) called for reductions in children's exposure to marketing of foods and non-alcoholic beverages high in saturated fat, salt and/or free sugars (HFSS) in all media and for the closing of regulatory loopholes to fully implement the WHO recommendations on marketing of food and non-alcoholic beverages to children (2). The Commission

made this call in light of unequivocal evidence that marketing influences dietary preferences, behaviours and childhood obesity, with implications for children's health and rights (3).²

In recent years, children's digital media use has expanded greatly, but policies to address marketing in these media have lagged behind those addressing marketing in “offline” traditional broadcast media. Indeed, existing policies (both regulatory

¹ The “black box” is a term frequently used to describe the “closed” nature of data in many digital (including social) media. See, for example, Pasquale F. *Black box society: the secret algorithms that control money and information*. Harvard: Harvard University Press; 2015.

² In line with WHO and United Nations practice, this paper defines “children” as those aged under 18 years.

and self-regulatory) have been criticized for weak controls over digital marketing (3). Online behavioural advertising, which permits advertisers to target individuals more effectively, is facilitated by collecting extensive personal data from Internet users, with fine-grained analyses of users' HFSS exposure and responses. There is currently little effective regulation to protect children – particularly adolescents – from digital HFSS behavioural advertising (3). Its extent, nature and impact on children is disputed: some industry players point to endemic online advertisement (ad) fraud, in a market where automated “bots” are known to inflate the number of visitors to sites to boost advertising revenue, and the lack of accurate measures of digital advertising “reach” (the number of people viewing an ad in digital media) (4). Others claim there is no evidence that children are indeed exposed to digital HFSS marketing at all (5). Yet, at the same time, brands and marketers consistently report that marketing for HFSS items amplifies traditional advertising, delivering increases in ad attention, recall, positive brand awareness and attitudes, intent to purchase and sales (3). Furthermore, social media advertising targeting tools, using online behavioural analysis, facilitate the targeting of children, making the ads potentially far more powerful.

Nevertheless, the extent of children's actual exposure to such marketing (and the persuasive techniques used) has not been identified through publicly available research, and privately owned digital media exclude external researchers from insights, reflecting inequity of access to data that is a widespread concern in this field (3). As children are avid users of digital media, and meta-analysis has established effects on their food preferences and dietary behaviours from television advertising and Internet advergames (6), specifying children's exposure to all HFSS marketing in digital media, and its power, is critical for researchers and regulators. Greater understanding of children's exposure (how much, where, and to what) and the persuasive techniques used will enable more targeted policy discussions and identification of appropriate entry points for regulations. Research identifying the extent, nature and impact of HFSS advertising in digital media to which children are exposed is therefore vital (3).

Digital media research presents particular, novel challenges, however, as methods remain to be developed, and accessing data from individuals and their digital devices “push[es] at the boundaries of existing research ethics guidance” (7, p. 1909). In addition, proposed methods have raised questions of legality within existing regulatory frameworks (7, 8), as well as within services' terms and conditions. Internet researchers adopt widely varying practices in data management, sharing and analysis; computing, data and analytics researchers have a higher tolerance for personal data extraction, use and analysis than social and behavioural

sciences researchers. There is little guidance to inform research and ethical design, and little evidence to guide institutional research review boards' risk identification and management (7, 8). Best practice and review processes are rarely shared publicly: researchers typically rely on informal exchanges of experience; indeed, they may experience post hoc ethical scrutiny in the peer-review process, which may hamper progress to publication (7). Furthermore, recent legal developments applicable to digital media research (such as those concerning the use of personal data for research purposes) require further attention.

WHO WORKSHOP ON DIGITAL HFSS MARKETING TO CHILDREN

To inform and support stakeholders in policy, research and ethics roles, the aim of this brief policy and practice paper is to summarize key ethical and legal issues when designing studies aiming to establish the extent, nature and impact of digital HFSS marketing to children. It builds on the conclusions of a two-day workshop in Copenhagen, Denmark, in November 2016, hosted by the WHO Regional Office for Europe's Division of Noncommunicable Diseases and Promoting Health through the Life-course, with attendees from Belgium, the Russian Federation, the United Kingdom and the WHO Regional Office for Europe including the paper's authors: researchers (Mimi Tatlow-Golden, Valerie Verdoodt, Emma Boyland, John Oates), including a research and Internet ethics expert (John Oates) and public health representatives (Jo Jewell, João Breda).

To guide workshop deliberations, the terms “marketing to children” and “marketing in digital media” were first defined (Table 1).

The workshop discussed two potential approaches to such research that would require collecting minors' social media and other online engagement data. The first involves use of competitive intelligence analysis, in which data regarding web traffic, social media brand mentions, target keywords and online advertising are assessed to identify brand performance. This widespread practice is standard in the marketing industry. It involves Internet platforms supplying – or analysts “scraping” – personal data, including data from minors, for a purpose users are unlikely to have envisaged when they engage with brands, peers or other content in social media, on video-sharing sites such as YouTube and on other Internet sites. Although the terms and conditions of many social media providers require users to agree to research on their data, it is unlikely that young users,

TABLE 1. DEFINITIONS OF MARKETING EMPLOYED TO GUIDE WORKSHOP DISCUSSIONS

Term	Definition
Marketing to children	Marketing to which children are actually exposed; analyses should not be limited to media overtly “targeted at” children but should also assess children’s exposure in general media.
Marketing in digital media	Digital marketing is promotional activity in digital media, maximizing impact with novel, creative and/or analytical methods, including: <ul style="list-style-type: none"> • creative and social methods to activate implicit emotional persuasion, including immersive narratives; entertainment/humour; augmented reality, online games and virtual environments; social network engagement (e-Word-of-Mouth); and “influencers” popular with children (such as YouTube video bloggers); • analytics of online behaviours to hone marketing communications and maximize impact; and/or • analytics of emotions, responses, preferences, behaviour and locations, to target specific groups, individuals and moments of vulnerability.

or indeed their parents/guardians, will be aware that they have consented to such practices. Such data collection is widespread in the commercial field but falls outside modes that research ethics review boards typically deal with.

The second option explored was a technology solution, an application (app) or virtual private network through which children’s Internet use can be recorded, with their and (where relevant) their parents’ or guardians’ consent, with the aim of identifying their advertising exposure in the context of individuals’ overall Internet use. Here, personal data (all traffic through their laptops or mobile devices) are accessed and uploaded to a secure site; relevant content is retained for analysis and non-relevant content discarded.

Both instances involve engaging with minors’ Internet data and, although focused on advertising exposure, may also extract information that is potentially sensitive and/or data from others in users’ networks who have not consented to take part, even if these were not the target data sought. The workshop addressed these and other challenges in the context of digital ethics guidance, European Union (EU) law and terms and conditions of social media platforms.

ETHICAL PRINCIPLES AND THE LAW

Four documents supported workshop deliberations: the recommendations of the ethics working committee of the Association of Internet Researchers (AoIR) (9); the European Data Protection Supervisor’s Opinion 4/2015 *Towards a new digital ethics* (10); the European Federation of Psychologists’ Associations Meta-code of Ethics (11); and the British Psychological Society’s ethics guidelines for Internet-mediated

research (12) – one of the few examples of Internet-specific research guidance from a professional association. These reiterate research ethics principles articulated in international policies (the United Nations Declaration of Human Rights, Nuremberg Code, Declaration of Helsinki and Belmont Report): respect for the fundamental rights of human dignity, autonomy, protection and safety, and the maximization of benefits and minimization of harms. They have a significant impact by shaping the actions of researchers, imposing limitations and offering guidance for research development and design. They also provide the basis for relevant legislation and normative guidance in its interpretation.

Ethics and the law share common ground to the extent that both are concerned with the nature of and maintenance of standards of human behaviour. However, not only do the law and ethics differ in important respects, they may also at times come into conflict. Whereas laws generally consist of a body of rules seeking to clearly define actions that are illegal and hence subject to prosecution, ethics generally consist of a set of moral principles, commonly understood as cohering around beneficence (benefit others) and non-maleficence (do no harm). In human research, ethical principles may, occasionally, motivate researchers towards actions that contravene a law. For example, a law requiring freedom of information may cause problems for a researcher who has established information about a participant that has clear potential for harm if disclosed. In contrast, acts that might be judged unethical, such as scraping extensive personal data from social media accounts where the media user has ticked to “accept” a multipage set of conditions without reading them, may nevertheless be lawful. Furthermore, an act that may be unlawful, such as engaging in research that contravenes aspects of social media services’ terms and conditions, may nevertheless be ethical, as it could generate information that may contribute to well-being. However, the formal regulatory setting for carrying out research activities is

provided by existing law, and therefore ethics, the law and their interaction must all be considered in the design of new methods.

The AoIR recommendations (9) argue that “all digital information at some point involves individuals”; therefore, “even if it is not immediately apparent how and where persons are involved”, it is likely that human subjects research principles must be considered. Critically, in this new and emergent field, Internet researchers are recommended by multiple guidelines to design studies for ethical compliance from ethical first principles and on a case-by-case basis. Similarly, AoIR argues that in this new territory a “dialogic, case-based, inductive, and process approach”, grounded in concepts such as harm, vulnerability, respect for persons and beneficence, is required (9, p. 5), cautioning that “ambiguity and uncertainty are part of the process”.

From a legal perspective, research employing personal data of EU citizens will need to meet requirements of the EU General Data Protection Regulation (GDPR) from 25 May 2018, including, where required, legal requirements regarding cross-border transfer of data. The GDPR includes provisions to better inform and protect users regarding personal data collection; procedures apply to all scientific research that employs personal data (such as epidemiology, clinical trials, public health and the

social sciences). It recognizes scientific research as a specific personal data-processing context requiring a balance between appropriate protection of individuals and information sharing in pursuit of the public interest (13), and thus adopts a new risk-based approach, with a case-by-case identification of data protection issues – in line with the AoIR recommendations. Importantly, the European Data Protection Supervisor’s Opinion 4/2015 further notes that legal adherence is not sufficient – ethical dimensions of data processing must also be addressed, including fundamental rights to privacy and to the protection of personal data enshrined in EU treaties, the EU Charter of Fundamental Rights and the Charter’s data protection principles. Key principles of “necessity, proportionality, fairness, data minimization, purpose limitation, consent and transparency” apply to all data collection and use (10). How these principles are to be applied in the context of Internet research, and particularly when it involves minors’ data, remains to be clearly articulated.

As a first indication of the key principles for Internet research, Table 2 shows those articulated in the British Psychological Society’s guidelines (12) and the considerations associated with them. For reasons of space in this short policy report the authors do not expand on these further here but refer researchers to the guidelines and to the increasing body of commentary in the field (see, for

TABLE 2. ETHICAL PRINCIPLES AND KEY CONSIDERATIONS OUTLINED IN THE BRITISH PSYCHOLOGICAL SOCIETY’S GUIDELINES

Principle	Considerations
Respect for the autonomy, privacy and dignity of individuals and communities	<p>Public/private distinction – the extent to which potential data derived from online sources should be considered in the public or private domain</p> <p>Confidentiality – levels of risk to the confidentiality of participants’ data, and how to minimize and/or inform participants of these risks, particularly where they may potentially lead to harm</p> <p>Copyright – copyright issues and data ownership, and when permission should be sought to use potential data sources</p> <p>Valid consent – how to implement robust, traceable valid consent procedures</p> <p>Withdrawal – how to implement robust procedures which allow participants to act on their rights to withdraw data</p> <p>Debriefing – how to implement robust procedures which maximize the likelihood of participants receiving appropriate debrief information</p>
Scientific integrity	Levels of control – how reduced levels of control may affect the scientific value of a study, and how best to maximize levels of control where possible
Social responsibility	Disruption of social structures – the extent to which proposed research study procedures and dissemination might disrupt/ harm social groups
Maximizing benefits and minimizing harm	<p>Maximizing benefits – how each of the issues mentioned above might act to reduce the benefits of a piece of research, and the best procedures for maximizing benefits</p> <p>Minimizing harm – how each of the issues mentioned above might lead to potential harm, and the best procedures for minimizing it</p>
<i>Source:</i> British Psychological Society (12).	

example, Samuel (14) and Gelinis et al. (15)). The principles and considerations summarized here guided the workshop discussion.

It is important to bear in mind that despite the stringent privacy protections of the GDPR, research participants' rights are not absolute – they are balanced with the risks and benefits of proposed research studies, requiring qualitative judgements to be made, in an ongoing process. Thus, ethics should not be addressed as a “regulatory hurdle”; rather, ethical enquiry requires ongoing deliberation (9).

Key factors to consider regarding this process and the case-by-case approach to ethics governance, summarized from the AoIR guidelines, are presented in Table 3. Again, this short commentary does not allow further expansion on these, but the interested reader is referred to the background discussion in the AoIR guidelines (9).

KEY ETHICAL AND LEGAL ISSUES TO CONSIDER

The workshop drew conclusions regarding key legal and ethical issues to be addressed when designing digital media studies involving data from those under 18 years; these are summarized below.

LAWFULNESS OF PROCESSING

Research organizations in and outside the EU that deal with data of EU individuals must follow GDPR requirements set out in its articles and recitals. For any personal data processing, the Regulation requires legitimate grounds. If research is the primary purpose of the personal data collection, three grounds for

processing might be relied upon (16): the data subject's consent, public interest and the legitimate interest of the controller (unless the controller is a public body). If research is not the primary purpose of the personal data collection – for example, if they were collected for another purpose but are now further processed for research purposes – this should be considered “compatible reuse” of personal data, implying that the same legal ground for processing can be used as for the initial processing (Recital 50). In this regard, appropriate safeguards should be in place, including pseudonymization (Article 89). Anonymity and confidentiality are key requirements, including effectiveness of de-identification and protection against capacity for re-identification.

DATA SUBJECTS' RIGHTS IN THE RESEARCH CONTEXT

Under the GDPR, data subjects' rights may present additional challenges: participants have a right to be informed and the Regulation contains notice requirements for the processing of personal data. For research-related processing, however, the GDPR relaxes the specificity of notice required – for example, requiring consent only for certain areas or parts of research projects (Recital 33). No notice is required for processing publicly available data, if provision of information would be impossible or would require a disproportionate effort, or if notice would render the research objective impossible or seriously impair it (Article 14(b)). However, it should be noted that “disproportionate effort” remains to be defined and that data subjects have a right to object to any personal data processing for research purposes, on grounds relating to their particular situation (Article 21(6)). Finally, with regard to data subjects' right to erasure, the GDPR allows exemptions for research under certain conditions (Article 17(3)). Overall, therefore, it makes considerable allowance for research-related data processing.

TABLE 3. KEY FACTORS TO CONSIDER, DRAWN FROM THE AOIR GUIDELINES

Factor	Considerations
Consult and deliberate	Ethical decision-making is a deliberative process. Researchers should consult widely, including researchers, people familiar with contexts/sites being studied, research review/ethics boards, guidelines, published scholarship in various disciplines and, where applicable, legal precedent.
A balance of rights	Researchers must balance their rights to conduct research and its social benefits with rights of authors/research participants. Participants' rights may outweigh research benefits.
Vulnerability	The greater the vulnerability of the community, author or participant, the greater the researcher's obligation to protect them.
Harm	“Harm” is defined contextually. Ethical principles are more likely to be applied inductively than universally, and ethical decision-making is best achieved with practical, context-sensitive judgement.
Not a one-off moment	Ethical issues need to be addressed at all steps of the research process: planning, research conduct, publication and dissemination.
<i>Source:</i> AoIR (9).	

PERSONAL OR PUBLIC DATA

One of the most challenging issues, which remains under discussion (17), is the question of when Internet data may be considered public (rather than private) and therefore reasonably processed without users' awareness or consent. It is important to note that even if social media data are legally public according to the terms of Internet platforms, people may have reasonable expectations of privacy. Gelinias and colleagues propose that data are private when users require a user name and password (15), yet research ethics committees have diverse views on this issue (14) and many social media platforms that require sign-in may generate publicly accessible data. For "big data" analyses, Nissenbaum has proposed the concept of "contextual integrity" (17), arguing that all social norms, including information norms, are contextual and change over time and location (9, 17). However, contextual integrity in the context of *children's* use of social media has not been defined, to the authors' knowledge. Although arguments are regularly made by Internet and social media platforms that younger people are no longer interested in privacy, the evidence shows that children are not familiar with the contents of privacy policies and struggle to understand them (18). A more persuasive argument emerging from research in Europe and the United States of America is that adolescents accept that data sharing is a precondition to participation in their peer networks, but carefully manage their online identities and social reputations (3). Therefore, these factors require consideration as part of ethical practice and the avoidance of harm. Finally, data from others in the networks of those who have consented to research participation – i.e. "bystander" data – should be accounted for and procedures articulated.

SENSITIVE INFORMATION

Information extracted may prove reputationally damaging if, for instance, it might be used to analyse children's engagement with alcohol advertising, or might yield data regarding other sensitive topics. The risk/harm balance should be carefully considered. From a legal perspective, sensitive data form a subcategory of personal data (such as racial or ethnic origin, religious preference, genetic data and so on), which can be processed lawfully for research purposes, if appropriate safeguards are in place (Article 9(2)(j)).

SAFEGUARDING

Researchers exploring social media data, especially those generated by minors or other vulnerable people, need to have in place protocols for managing risks of uncovering evidence of criminal or other harmful activity that may, depending on local legal frameworks, impel them to take actions that would breach generic confidentiality conditions, such as informing police, health or other relevant authorities. For example, risks

can include evidence of physical or sexual abuse, serious mental health issues, or radicalization for terrorism.

SECURITY IN DATA PROCESSING (STORAGE, CLASSIFICATION, MANAGEMENT); DATA SHARING (INCLUDING CROSS-BORDER)

A level of security appropriate to the risk (Article 24) should be ensured, and data only stored in a form which permits identification for as long as necessary (Article 5(c)). Transfers of personal data to third countries or international organizations must comply with GDPR requirements.

PARTICIPATION: AGE OF CONSENT

The age at which children/young people may legally consent to taking part in research on their own behalf varies across jurisdictions.

CONSENT TO PARTICIPATE AND WITHDRAWAL PROCEDURES, INCLUDING "INFORMED" VERSUS "VALID" CONSENT

Where data from minors are concerned, the imperative to act transparently and minimize harm is sharpened. Although there may be instances where gaining consent is challenging, it is preferable to do so where possible. Verbal and written descriptions of consent conditions need to be carefully tailored to the literacy and cognitive levels of child participants. Procedures for withdrawal from a study need to be clearly articulated, including the implications for data removal on request. It is especially important to ensure that children do not feel implicit coercion to participate in a study, or to continue to participate when they no longer wish to. It should be noted that whereas consent is often framed as "informed", increasingly the term "valid" is considered more appropriate (12), because fully informed consent at the start of involvement in a study is rarely feasible not only for children but indeed also for adults. As with the ongoing ethical process itself, consent should be also viewed as ongoing: children's attitudes to data being collected from them may change as they find out more by participating in a research study.

ACCURACY/JUSTICE IN PARTICIPANT SELECTION

Ethical issues of justice regarding representation of less advantaged communities may arise due to sampling biases inherent in some digital and Internet research (20, 7). For example, children may not have their own digital devices such as smartphone or tablet (they may share access to one within the family) and the data- and generalisability-related implications should be factored in.

SOCIAL NETWORKS AND APP STORES: TERMS AND CONDITIONS

The workshop's conclusions also summarized the multiple layers of legal requirements involved if aiming to access and use content or features of a social network platform. Researchers developing an app to access a platform's content through the app programming interface (API: a set of functions and procedures designed to allow such access) must abide by the platform's terms and conditions, a legal contract defining, *inter alia*, obligations, restrictions (for example, most stipulate that data obtained may not be sold for commercial purposes), requirements for user protection and warranty disclaimers. Terms of use are generally non-negotiable, and developers enter into the contract by accession (by using the platform's content or features); best intentions to comply might not always be sufficient, as terms and conditions are often vague (19), allowing platform providers to interpret any ambiguities to their own advantage if legal conflicts arise. Furthermore, social media platforms usually reserve the right to modify API terms and conditions unilaterally, sometimes without informing developers – whose continued use of platforms' content and features indicates they agree with any changes. If the platform suspects any breaches of terms and conditions, access to the API will be cut, although recently the European Commission recognized that this may constitute an unfair trading practice (21). Developers therefore need to follow up continuously on compliance with API terms and conditions. Notably, there is currently no exception to these rules for research purposes (19).

Smartphones or tablets use specific operating systems requiring download of apps through stores online (such as the Apple or Google Play stores for Apple and Android devices, respectively), which have their own terms and conditions. Developers need to submit apps for review having addressed app stores' technical content and design criteria. Legal requirements relate mostly to customer privacy and personal data protection (such as data storage, data use and sharing and children's data) and compliance with national intellectual property legislation, ensuring apps only include original or licensed content. Apps using content without permission are usually removed by the app store.

CONCLUSION

In sum, the requirements of ethical research procedures, as well as of the formal legal requirements of the GDPR, necessitate a nuanced, case-by-case consideration of the balance of harms and benefits that research provides. As the GDPR articulates stringent requirements regarding the protection of personal data yet also recognizes the needs of researchers and benefits to

society of meaningful research, each research case will need to be considered on its merits. The issue of consent raises specific ethical and legal issues (including consent to participation in research, legal age of consent and consent as a potential ground legitimizing the processing of personal data). Wherever possible, consent should be incorporated not as a one-off event but as a process. Despite these important considerations, the workshop panel concluded that research projects such as those indicated above satisfied the conditions of benefit to society, and that therefore invoking ethical principles to block such research would itself be unethical.

Nevertheless, it is of note that complex legal conditions are set by digital platforms themselves – which, unlike the GDPR, do not contain a research exception for purposes other than internal research. This adds to the ethical–legal hurdles faced by researchers seeking to identify solutions to this pressing public health concern. The authors are aware of instances in which research ethics committees have chosen to recommend that institutions support studies that breach social media platforms' terms and conditions and to indemnify researchers carrying out these studies. This is under the assumption that the risk to the institution is low, as it is unlikely that powerful Internet stakeholders such as social media providers would seek to pursue public health researchers who contravene these conditions, as substantial adverse publicity could be expected given that genuine social benefit would accrue from such research.

Research providing objective data on children's actual exposure to digital marketing, and essential information about the persuasive techniques used, will clarify what types of marketing children see and where, and provide more concrete evidence of the problem. This will be important for regulatory agencies in designing regulatory interventions (choosing what to specify in the rules) and identifying the most appropriate regulatory entry point (recommending which agency or authority is best placed to develop, oversee and enforce the rules). It would therefore contribute hugely to the richness of policy discussions and should be prioritized as a research goal.

Sources of funding: Valerie Verdoodt's contribution for this article was funded and created in the context of the AdLit Project, Research Fund Flanders. No other sources of funding were declared.

Conflicts of interest: None declared.

Disclaimer: The authors alone are responsible for the views expressed in this publication and they do not necessarily

represent the decisions or policies of the World Health Organization

REFERENCES

1. Commission on Ending Childhood Obesity. Report of the Commission on Ending Childhood Obesity. Geneva: World Health Organization; 2016 (<http://www.who.int/end-childhood-obesity/publications/echo-report/en/>, accessed 20 November 2017).
2. Set of recommendations on the marketing of food and non-alcoholic beverages to children. Geneva: World Health Organization; 2010 (<http://www.who.int/dietphysicalactivity/publications/recsmarketing/en/>, accessed 20 November 2017).
3. Tackling food marketing to children in a digital world: trans-disciplinary perspectives. Children's rights, evidence of impact, methodological challenges, regulatory options and policy implications for the WHO European Region. Geneva: World Health Organization; 2016 (<http://www.euro.who.int/en/health-topics/disease-prevention/nutrition/publications/2016/tackling-food-marketing-to-children-in-a-digital-world-trans-disciplinary-perspectives.-childrens-rights,-evidence-of-impact,-methodological-challenges,-regulatory-options-and-policy-implications-for-the-who-european-region-2016>, accessed 20 November 2017).
4. Cookson R. Digital advertising: brands versus bots. *Financial Times*. 2016; 18 July (<https://www.ft.com/content/fb66c818-49a4-11e6-b387-64ab0a67014c>, accessed 20 November 2017).
5. Clarke B, Svanaes S. Literature review of research on online food and beverage marketing to children. Produced for the Committee of Advertising Practice. London: Family Kids & Youth Market Research and Consultancy; 2014 (<https://www.asa.org.uk/resource/CAP-response-to-the-Family-Kids-&-Youth-Review.html>, accessed 20 November 2017).
6. Boyland EJ, Nolan S, Kelly B, Tudur-Smith C, Jones A, Halford JC et al. Advertising as a cue to consume: a systematic review and meta-analysis of the effects of acute exposure to unhealthy food and nonalcoholic beverage advertising on intake in children and adults. *Am J Clin Nutr*. 2016; 103(2):519–33. doi:10.3945/ajcn.115.120022.
7. Shilton K, Sayles S. "We aren't all going to be on the same page about ethics": ethical practices and challenges in research on digital and social media. 49th Hawaii International Conference on System Sciences, Kauai, Hawaii, 5–8 January 2016. Piscataway, NJ: Institute of Electrical and Electronics Engineers; 2016:1909–18.
8. Weller K, Kinder-Kurlanda KE. Uncovering the challenges in collection, sharing and documentation: the hidden data of social media research? In: Proceedings. Standards and practices in large-scale social media research. Ninth International AAAI Conference on Web and Social Media, Oxford, United Kingdom, 26–29 May 2015. Palo Alto, CA: Association for the Advancement of Artificial Intelligence; 2015:28–37.
9. Ethical decision-making and Internet research: recommendations from the AoIR ethics working committee. Chicago, IL: Association of Internet Researchers; 2012 (<https://aoir.org/ethics/>, accessed 20 November 2017).
10. Towards a new digital ethics: data, dignity and technology. Brussels: European Data Protection Supervisor; 2015 (Opinion 4/2015; https://edps.europa.eu/data-protection/our-work/publications/opinions/towards-new-digital-ethics-data-dignity-and_en, accessed 20 November 2017).
11. Meta-code of Ethics. Brussels: European Federation of Psychologists' Associations; 2005 (http://www.bdp-verband.org/bdp-verband/clips/efpa_metacode_en.pdf, accessed 27 November 2017).
12. Ethics guidelines for Internet-mediated research. Leicester: British Psychological Society; 2017 (INF206/04.2017; <https://beta.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research-2017>, accessed 20 November 2017).
13. Chassang G. The impact of the EU general data protection regulation on scientific research. *Ecancermedicallscience*. 2017; 11:709. doi:10.3332/ecancer.2017.709.
14. Samuel G. "The danger of lurking": different conceptualizations of "user awareness" in social media research. *Am J Bioeth*. 2017; 17(3):25–6.
15. Gelinis L, Pierce R, Winkler S, Cohen IG, Lynch HF, Bierer BE. Using social media as a research recruitment tool: ethical issues and recommendations. *Am J Bioeth*. 2017; 17(3):3–14.
16. Bird & Bird, Taylor M. Analysis: research and the General Data Protection Regulation – 2012/0011(COD). Edinburgh: University of Edinburgh; 2016 ([http://www.research.ed.ac.uk/portal/en/publications/analysis-research-and-the-general-data-protection-regulation--20120011cod\(1ad0efb6-55bb-4af3-b37a-fb1e1c8642d2\).html](http://www.research.ed.ac.uk/portal/en/publications/analysis-research-and-the-general-data-protection-regulation--20120011cod(1ad0efb6-55bb-4af3-b37a-fb1e1c8642d2).html), accessed 20 November 2017).
17. Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press; 2010.
18. Growing up digital: a report of the Growing Up Digital Taskforce. London: Children's Commissioner for England; 2016 (<https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/>, accessed 20 November 2017).

-
19. Kuczerawy A. The perils of app development – compliance with API terms & conditions [blog post]. Leuven: CiTiP Blog (KU Leuven); 2016 (<https://www.law.kuleuven.be/citip/blog/the-perils-of-app-development-compliance-with-api-terms-conditions/>, accessed 20 November 2017).
 20. Boyd D, Crawford K. Critical questions for big data. *Inf Commun Soc.* 2016; 15:662–79.
 21. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online platforms and the digital single market, opportunities and challenges for Europe. Brussels: European Commission; 2016 (<https://ec.europa.eu/digital-single-market/en/policies/online-platforms>, accessed 20 November 2017). ■