Dear Senators

Thank you for the opportunity to provide additional information in relation to privacy issues within the context of the games industry and, in particular, what best practice in privacy could look like. There are three key areas where Australia could improve if we were to strive for best practice. We touch on each of these briefly below, so as to close the loop on the question raised during the hearing:

1. **Parental consent for collection of children's data**: At present Australia does not have any laws specifically addressing the privacy of children online. No jurisdiction can easily be identified as having best practice on this issue, but the USA has addressed concerns via its *Children's Online Privacy Protection Act* of 1998 (COPPA). There are issues with COPPA, particularly as the original laws were not technology neutral (they were focussed on websites) and therefore do not easily transport into new technologies (such as smart phones). However the requirement of verifiable parental consent is a strong foundation for protection.

2. **Data profiling**: please find attached an article on the proposed EU laws relating to data profiling. We encourage the Australian government to monitor the issue of profiling and remain in-step with advancements in Europe in this area.

3. **Right to be forgotten:** in Australia, an individual cannot easily require another person or company to remove or delete their personal information. The ability for an individual to be able to control their personal information has proved to be a powerful right in Europe, where the tort first arose in 2010 (http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf). Such a right, would be an important improvement to the rights of Australian citizens who at present must rely on copyright, confidentiality or defamation legal heads to seek redress – none of which adequately provide a solution. Such a right would be much more valuable to Australians than the proposed data breach notification regime. Much work has already gone into designing what such a statutory right would look like in Australia:

    a. Australian Law Reform Commission Report (2014): https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123
    b. South Australian Law Reform Institute (2016): https://law.adelaide.edu.au/research/law-reform-institute/documents/privacy_final_report_4.pdf
    c. NSW Legislative Council inquiry into Remedies for the serious invasion of Privacy in NSW (2016): http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/0F02A41F813CF811CA257F6A007F7BB2?open&refnavid=CO3_1

We thank you for the opportunity to provide this further information and to participate in the Inquiry.

Kind regards
Kate Hynes

Kate Hynes
Chief Legal Officer

HALFBRICK

23 Musgrave Road
Red Hill
QLD 4059 Australia **web:** www.halfbrick.com

The Privacy Advisor

Original reporting and feature articles on the latest privacy developments

Top 10 operational impacts of the GDPR: Part 5 - Profiling

Rita Heimes
The Privacy Advisor | Westin Research Center | Jan 20, 2016

The new General Data Protection Regulation (GDPR), put forth by the European Commission in 2012 and finally generally agreed upon by the European Parliament and Council in December 2015, is set to replace the Data Protection Directive 95/46/ec. Once the GDPR is formally adopted by the European Parliament and Council and printed in the Official Journal of the European Union sometime this spring, it will be directly applicable in each member state and lead to a greater degree of data protection harmonization across EU nations.

Although many companies have already adopted privacy processes and procedures consistent with the Directive, the GDPR contains a number of new protections for EU data subjects and threatens significant fines and penalties for non-compliant data controllers and processors once it comes into force in the spring of 2018.

With new obligations on such matters as data subject consent, data anonymization, breach notification, trans-border data transfers, and appointment of data protection officers, to name a few, the GDPR requires companies handling EU citizens' data to undertake major operational reform.

This is the fifth in a series of articles addressing the top 10 operational impacts of the GDPR.

The GDPR restricts "profiling" and gives

data subjects significant rights to avoid profiling-based decisions

Since the Directive was implemented nearly 20 years ago, technologies have proliferated that allow data controllers to gather personal data and analyze it for a variety of purposes, including drawing conclusions about data subjects and potentially taking action in response to those conclusions such as target marketing, price differentiation, and the like. Although the concepts of "profiling" or "target marketing" appear in the Directive, the precise terms do not. In its sweeping efforts to define and enhance data subjects' rights to control their personal data, the GDPR contains many restrictions on automated data processing – and decisions based upon such processing – to the extent they can be characterized as profiling.

Definition of profiling

A hotly contested provision of the GDPR, the "profiling" restrictions ultimately adopted were narrower than initially proposed.

Under Article 4(3aa), data processing may be characterized as "profiling" when it involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Specific examples include analyzing or predicting "aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

This definition implicitly excludes data processing that is not "automated."

Further elaboration of this definition may be found in the Recitals, where the GDPR establishes its jurisdiction over non-EU controllers provided they are "monitoring the behaviour of [EU] data subjects as far as their behaviour takes places within the European Union." Processing activity involves data subject "monitoring" when "individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

This definition suggests that profiling is not equivalent to tracking, but instead is something more, involving the intention to *take decisions* regarding a data subject or *predict* the subject's behaviors and preferences.

That "profiling" requires some sort of an outcome or action resulting from the data processing is underscored by the data subject's rights to be informed of the "consequences" of profiling decisions as discussed in Recitals 48 and 51. Articles 14 and 15, which address information to be provided a data subject upon personal data collection and upon the data subject's request, both require disclosure of "the existence of automated decision making including profiling" along with "the significance and the envisaged consequences of such processing for the data subject."

Elsewhere in the Recitals, data subjects are given the right to object to processing for direct marketing as well as to "profiling to the extent it is related to direct marketing," further underscoring that profiling is not direct marketing *per se* but instead is something more.

Finally, Recital 71 describes the obligation to conduct a data impact assessment and characterizes the "profiling of data" as follows: "A data protection impact assessment should also be made in cases where data are *processed for taking decisions* regarding specific individuals *following any systematic and extensive evaluation of personal aspects relating to natural persons* based on profiling those data."

Accordingly, taking all of the definitions and discussions of "profiling" together, they seem to consistently require not simply the gathering of personal data involving personal aspects of natural persons, but the automated processing of such data for the purpose of making decisions about the data subjects.

Controllers must honor data subjects' rights regarding profiling

Data subjects are entitled under the GDPR to a number of rights with regard to profiling, some of which – like notice and access – require procedures similar to non-profiling data processing, but others of which – like the right to object, halt the profiling, and avoid profiling-based decisions – will require special attention

and processes for compliance.

Restrictions on profiling-based decisions producing legal effects

Pursuant to Article 14(1) of the GDPR, data subjects have a right not necessarily to avoid profiling itself (e.g. automated processing of personal data for the purpose of making a decision), but rather to avoid being "subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Recital 58 provides as examples the "automatic refusal of an on-line credit application or e-recruiting practices without any human intervention."

Article 14(1a) clarifies that the *decision* may nonetheless be made provided it is (a) necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) authorized by Union or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) based on the data subject's explicit consent. Suitable safeguards may include anonymization or pseudonymization as components of profiling-based activities.

In the case of a decision made pursuant to a contract with the data subject or his explicit consent, the controller must still allow the data subject to contest the decision under Article 20(1b).

When data is transferred pursuant to Binding Corporate Rules, such BCRs must specify "the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 20."

Article 20(3) provides that profiling-based decisions shall not be based on special categories of personal data (e.g. racial, ethnic, or religious information) unless (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where prohibited by Union law or member state law; or (b) processing is necessary for reasons of substantial public interest, on the basis of Union or member state law. Even in these circumstances,

described more fully in Article 9(2)(a) and (g), the controller must still ensure "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place." Presumably the European Data Protection Board will provide additional guidance on the circumstances under which profiling-based decisions are permissible for special categories of personal data.

For all permissible profiling, Recital 58 compels a controller to use adequate mathematical or statistical procedures, implement technical and organisational measures to correct data inaccuracies and avoid errors, secure all personal data, and minimize the risk of "discriminatory effects against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, or sexual orientation."

Notice and access

In the case of profiling decisions subject to Article 20, Article 14 provides that the controller must inform a data subject at the time data is collected not only of the fact that profiling will occur, but as well "the logic involved" and "the envisaged consequences of such processing." Under Article 15, a data subject may also inquire of a controller and receive confirmation of any such processing, including profiling and its consequences, at any time.

Processing must cease upon data subject's objection

Even when profiling is otherwise lawful, a data subject has the right to object at any time. Pursuant to Article 19, upon the data subject's objection to profiling that is otherwise authorized under Article 6, the processing must cease unless the controller demonstrates "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject."

When processing is for direct marketing purposes, including profiling, the data subject similarly has a right to object but in this case processing must cease and the controller is not authorized to continue under any circumstances.

Data impact assessments for controllers engaged in profiling

One of the triggers requiring a data impact assessment is when a controller engages in "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual." Parsing this language once again demonstrates that "profiling" involves more than merely automated processing, and that profiling may or may not involve decisions that produce legal effects or significantly affect an individual, but, when it does, the data subject is entitled to many additional rights and remedies.

Conclusion

Controllers will undoubtedly be seeking additional guidance from the European Data Protection Board to determine what automated data processing activities fall within the definition of profiling, and what profiling activities may fall outside the purview of Article 20. Data subjects, on the other hand, will benefit from a broader interpretation of profiling activities in order to be able to avoid profiling-based decisions – even those to which they have given prior explicit consent.

Photo credit: Egyptian via photopin (license)

Where to find the rules

Looking to dive deeper into the General Data Protection Regulation to read the text regarding profiling for yourself? Find the full text of the Regulation here in our Resource Center.

You'll want to focus on these portions:

Recitals

(21) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes places within the European Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(48) The principles of fair and transparent processing require that the data subject should be informed of the existence of the processing operation and its purposes. … Furthermore the data subject should be informed about the existence of profiling, and the consequences of such profiling. Where the data are collected from the data subject, the data subject should also be informed whether he or she is

obliged to provide the data and of the consequences, in cases he or she does not provide such data. …

(51) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, where possible for what period, which recipients receive the data, what is the logic involved in any automatic data processing and what might be, at least when based on profiling, the consequences of such processing. …

(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether the initial or further processing, at any time and free of charge. This right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(58) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' consisting in any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements as long as it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision making based on such processing, including profiling, should be allowed when expressly authorised by Union or Member State law, to which the controller is subject, including for fraud and tax evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of EU institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child, to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision. In order to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed, the controller should use adequate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure in particular that factors which result in data inaccuracies are corrected and the risk of errors is minimized, secure personal data in a way which takes account of the potential risks involved for the interests and rights of the data subject and which prevents inter alia discriminatory effects against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, sexual orientation or that result in measures having such effect. Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.

(59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, decisions based on profiling, as well as

on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or member state law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other public interests of the Union or of a member state, in particular an important economic or financial interest of the Union or of a member state, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes.…

(71) This should in particular apply to large-scale processing operations, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories ofpersonal data, biometric data, or data on criminal convictions and offences or related security measures. ….

Articles

Article 4, *Definitions* (3aa) 'profiling'

Article 6, *Lawfulness of processing*

Article 14, *Information to be provided where the data are collected from the data subject*

Article 15, *Right of access for the data subject*

Article 19, *Right to object*

Article 20, *Automated individual decision making, including profiling*

Article 33, *Data protection impact assessment*

Article 43, *Transfers by way of binding corporate rules*

Article 66, *Tasks of the European Data Protection Board*

1 Comments

Logged-in as: **Kate Hynes**

Share your thoughts

Lewis Barr • Jan 22, 2016

Excellent article, Rita. Thank you.