Cross device profiling — ensuring compliance

Bridget Treacy, Partner, and James Henderson, Associate, consider the compliance issues that arise from the use of techniques and algorithms enabling cross device profiling, and explain how organisations can ensure that they are sufficiently transparent with their use

Cross device profiling, the range of techniques that allows individual users to be identified across different devices and platforms, is now commonplace. In the past, organisations have relied on cookies and similar technologies to identify users. As the mobile ecosystem has become more sophisticated, and service offerings have been deployed on new platforms, organisations have turned to newer technologies to enable them to identify individual users across those platforms. It is now common for users to access a single service through multiple platforms, for example, a smartphone, tablet, laptop, and even smart televisions. Through cross device profiling, organisations can identify and target individual users more accurately than ever before, and provide increasingly personalised services.

However, the techniques and algorithms utilised to enable cross device profiling are often less than transparent, raising complaints from individuals that such practices are 'creepy' or intrusive. Such techniques have only recently begun to receive specific regulatory attention, but as awareness of individuals' privacy rights continues to grow, and those rights are further enhanced by the proposed General Data Protection Regulation, companies deploying these techniques will need to consider whether their practices are sufficiently transparent.

Accuracy of deterministic or probabilistic techniques

Organisations typically employ a range of techniques to achieve cross device 'identifiability'. These techniques may be deterministic (i.e. where the organisation uses a unique identifier to identify the user when he or she uses different devices) or probabilistic (i.e. where the organisation, typically through a combination of techniques, infers the identity of the user in question, through a range of factors and characteristics associated with his or her device or usage, such as IP address range, past browsing history, etc.).

Many profiling techniques will employ both deterministic and probabilistic methods. Commentators estimate that most probabilistic techniques have a level of accuracy of between 60-80%. This means in 20 — 40% of cases, organisations associate a range of inferred characteristics and behaviours with the incorrect user. Over time, these accuracy levels will undoubtedly improve, but the risks of error that currently exist make it imperative that organisations think carefully about data protection compliance now.

Data Protection Directive

The Data Protection Directive (95/46/EC) regulates the processing of 'personal data' by 'data controllers' that are established in the EU or employ equipment based in the EU for the purpose of processing personal data. If each of these three elements applies, then an organisation performing cross-device profiling will be subject to the compliance obligations set out in the Directive.

Are personal data being processed?

The definition of 'personal data' in the Directive captures any information that relates to an individual and which identifies an individual, or from which an individual may be identified. This definition is extremely broad and captures expressions of opinion about an individual, as well as factual statements, provided the information identifies the individual or the individual can be identified from the data.

Deterministic profiling measures typically utilise a unique identifier that is tied to a particular identified individual. Such an identifier clearly allows the particular user in question to be identified and singled out (indeed, this is the intention of profiling). Accordingly, that unique identifier, as well as any other data linked to that identifier (e.g., devices, IP address, browsing habits and history) will constitute personal data.

Probabilistic profiling techniques typically analyse vast sets of data

(Continued on page 10)

(Continued from page 9)

to identify particular users from that data. Once tied to a particular known (or suspected) individual, that data will constitute personal data. It should be noted that the data in question will also constitute personal data even if they are associated with the incorrect individual, provided an individual can be identified from those data.

Is processing conducted by a controller?

The second requirement is that the organisation conducting the profiling is a 'data controller' within the meaning of the Directive.

A data controller is a person who 'determines the purposes and the means of the processing of personal data'. Organisations that perform cross device profiling typically are data controllers, but organisations may perform cross device profiling on behalf of another website or service operator — in which case the website or service operator will be the data controller. Care is required to determine which entity is the data controller, and has the applicable legal compliance obligations under the Directive.

EU establishment

Assuming that an organisation processes personal data in the capacity of a data controller, the organisation will be subject to the Directive if it is established within the EU, or if it utilises equipment within the EU for the purpose of processing personal data. Organisations that are located within an EU Member State (either by a legal entity established in that jurisdiction, or some other physical presence) will be subject to the Directive as implemented in that Member State. It should be noted that the 'use of equipment' test is interpreted widely, and the mere placing of cookies on a user's equipment is likely to bring a non-EU data controller within scope of the Directive, even if they have no physical presence in the EU.

"In many cases, the nature of the profiling and the techniques deployed may not be transparent or understandable to data subjects, raising the risk that any consent is invalid. For consent to be valid, users must be given a genuinely free choice as to whether they are tracked, or not."

Legal basis for processing

Data controllers must satisfy one of the processing conditions set out in the Directive. In the context of cross-device profiling, the relevant conditions are consent, and the legitimate interests of the data controller. The contractual necessity ground will not usually be applicable, unless cross-device tracking is strictly necessary for provision of the service. This is a strict test, and will not apply to cross-device tracking carried out for purposes that are not strictly necessary, for example for the purpose of providing personalised services.

In many cases, organisations seek to rely on consent as the legal basis for cross-device profiling. The Data Protection Directive does not dictate the form by which consent is obtained, but consent must be freely given, specific and informed. This requirement has been interpreted differently across the Member States. In some jurisdictions, forms of implied consent (such as 'banner' systems deployed in the context of cookies) may be valid, and in some cases valid consent maybe obtained through web browser settings.

In the context of cross-device profiling, the key consideration is to ensure that data subjects are fully aware of what they are consenting to. Organisations should explain, in a user friendly and transparent manner, why profiling techniques are deployed. This is particularly important where the profiling techniques deployed may have a significant impact on the privacy of individuals or otherwise significantly affect them, for example, where differential pricing is used. In many cases, the nature of the profiling and the techniques deployed may not be transparent or understandable to data subjects, raising the risk that any consent is invalid. For consent to be valid, users must be given a genuinely free choice as to whether they are tracked, or not.

Alternatively, controllers may rely on their legitimate interests as a basis for cross device profiling, provided such legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject. The Article 29 Working Party has published an Opinion (copy available at: www.pdpjournals.com/docs/88446) on legitimate interests in which it set out a three-stage test to determine whether the legitimate interests basis is available in a particular context. In the context of online cross device tracking, the legitimate interests basis may be difficult to establish, as users may not be fully aware of the processing that takes place, and due to the broader privacy implications of being tracked across multiple devices.

Typically, data controllers rely on consent for cross device profiling, but care is needed to satisfy the requirements for consent outlined above.

Fair processing notice

Under the Directive, data controllers are required to provide notice to individuals as to how their personal data will be processed. At a minimum, this information includes the identity of the data controller (and its representative,

if established outside the EU), the purposes for which personal data will be processed, and information as to the recipients or categories of recipients to whom personal data will be disclosed.

In addition, the data controller is required to provide any further information that is necessary to guarantee fair processing of personal data. In the context of cross device profiling, the scope of such further information will require careful consideration, not least because this requirement has not been interpreted uniformly across the EU.

Perhaps the key compliance risk in this context, assuming that an adequate information notice has been prepared, is making the information available to data subjects in a fair and easily understandable manner. This can pose particular challenges where sophisticated tracking techniques are utilised. Data controllers must explain such techniques using clear language, free from technical jargon. Typically, information relating to cross device profiling would be included in the privacy notice placed on a website that utilises cross device profiling techniques.

Data subject rights

The Directive provides data subjects with certain rights in relation to the processing of personal data about them. These rights include the right of subject access, the right to be made aware of the logic involved in any automatic processing of personal data, the right to have inaccurate, irrelevant or out of date information blocked, rectified or erased, and the right to object to processing on compelling legitimate grounds. In addition, data subjects have the right not to be subject to decisions that significantly affect them that are based solely on automated processing of data.

Data controllers that are engaged in cross device profiling will need to be ready to comply with each of these requests. Of particular importance is the right to correct irrelevant, inaccurate or out of date personal data and the right to object to processing on compelling legitimate grounds.

In the case of probabilistic profiling, users should be given the right to disassociate their profile from the actions of other users, particularly where it is clear that the data controller has not accurately identified the individual in question. Various mechanisms may be deployed to enable controllers to honour these rights, but typically 'dashboard' style systems that enable a high degree of transparency over the precise categories of data that are used to build the user's profile, as well as the opportunity to access, correct and block those data at a granular level, enable better compliance.

E-Privacy Directive

The e-Privacy Directive requires that an individual's informed consent is obtained before information can be stored on, or accessed from, their terminal equipment. Often referred to as the 'cookie law', the language of the e-Privacy Directive extends beyond cookies and includes all technologies that either store information on or read information from a user's device, including web based services and applications. The specific type of cross device tracking technology to be deployed will need to be analysed carefully, but it is likely that many (or perhaps most) of these technologies will fall within the scope of the e-Privacy Directive. Further, it is unlikely that the exemption to consent, where the technology is strictly necessary in order to provide a requested service, will apply to cross device tracking. Typically, cross device tracking enables additional, value added, personalised or tailored content, but in most cases this will not be 'strictly necessary' in order to provide the core service.

Organisations will need to think carefully about how they obtain any required consent. Guidance has been provided by the Article 29 Working Party in Working Document 02/2013 (copy available at: www.pdpjournals.com/docs/88441) on obtaining consent to the use of cookies. In that guidance, the Working Party notes that consent must be given before any data processing begins. This means that cross device tracking technologies that are subject to the e-Privacy Directive should only be activated after the user has been provided with relevant information, and given the opportunity to accept or decline the use of the tracking technology. The Working Party reiterates in the guidance its view that valid consent requires that a user is given a free and active choice. Any consent must constitute an active indication of the user's wishes, although the means by which consent is given is not prescribed. This requirement has been interpreted differently across the EU, but many Member States accept that implied consent (for example, inferred from a user's failure to navigate away from the site in question, after having been provided with clear notice of the use of cookies) is sufficient. Data controllers engaged in cross device profiling will need to consider these requirements in each Member State in which they operate.

Proposed General Data Protection Regulation

The proposed EU General Data Protection Regulation is expected to result in significant changes for organisations that carry out cross device profiling. The final text of the Regulation is still being negotiated by the EU institutions. It is expected to be agreed in late 2015, and to enter into force in 2017. However, a number of key concepts and proposed changes appear to be accepted, in principle, by the respective institutions.

The territorial scope of the Regulation will almost certainly be wider than under the Directive. The 'equipment test', described above, will be replaced by a test that focuses on whether the data controller monitors the behaviour of EU residents. Organisations (possibly processors as well as controllers) that monitor EU-based users' behaviour for the purpose of identifying them across devices will fall within scope of the Regulation. Whereas under the Directive organisations may have been able to argue that the 'equipment test' did not apply, this argument will be even more difficult to sustain under the Regulation.

(Continued on page 12)

(Continued from page 11)

The second key change concerns the definition of 'personal data'. The Regulation will specifically include 'online identifiers' within the categories of personal data. Most forms of deterministic profiling that utilise a unique user identifier will be personal data under the Directive, but this will be put beyond doubt in the Regulation. This change in the definition of personal data will not specifically affect forms of probabilistic profiling, but where an individual can be identified, then the Regulation will apply, just as the Directive does at present.

Under the Regulation, profiling will for the first time be specifically regulated. The Regulation defines profiling as processing intended to 'evaluate, analyse or predict any feature of [the data subject's] behaviour, preferences or identity'. This definition is cast extremely widely, and would clearly capture cross device profiling that attempts to infer the identity of a particular user through the evaluation and analysis of their online behaviour and characteristics.

The Regulation will prohibit all forms of profiling that produce 'legal effects' or otherwise 'significantly affect' the data subjects that are profiled. Although these terms are not defined, they are likely to be interpreted widely, for example, to include personalised ads served on the basis of the identity of the user, or differential pricing offered on the basis of the particular user in question. It is as yet unclear whether less privacy intrusive profiling use cases would be captured, for instance cross device profiling carried out for the purposes of providing personalised services to a particular user on the basis of the device they are using.

Profiling that produces a legal effect or otherwise significantly affects data subjects will be prohibited subject to limited exemptions, the primary one being that the profiling is carried out with the consent of data subjects. Under the Regulation, such consent will need to be 'explicit' in order to be valid. In practice this requirement will mean that mere acquiescence on the part of data subjects (for example, failing to un-tick a pre-ticked box, or failing to navigate away from a website) is unlikely to constitute valid consent. All organisations that carry out cross device profiling will need to review their consent mechanisms to ensure they will remain valid under the Regulation, particularly those that currently rely on forms of implied consent.

The scope of the legitimate interests processing ground under the Regulation is not yet clear. If legitimate interests is no longer available, consent is likely to be the next best option to consider. It is also unclear whether profiling based solely on categories of sensitive data will be prohibited, or permitted with data subject consent.

Finally, it should be noted that the Regulation will significantly increase the applicable penalties for non-compliance, with fines of up to 5% of global revenue under discussion. It is as yet unclear how such fines will be applied, but the order of magnitude represents a significant departure from the position under the Directive.

Conclusion

Cross device profiling poses significant compliance risks under the Directive and the e-Privacy Directive. In particular, organisations will need to ensure they have a valid legal basis on which to conduct cross device profiling, and that appropriate, clear information is provided about the processing activities. Ensuring that data subject rights can be accommodated may pose particular difficulties in the cross device profiling context.

More generally, cross device profiling has received little specific regulatory attention to date (other than in the context of cookies), and there has been little or no enforcement action on these issues to date. Whether this position changes in future will remain to be seen, but profiling seems likely to be subject to increased scrutiny under the proposed Data Protection Regulation.

Bridget Treacy and James Henderson
Hunton & Williams
btreacy@hunton.com
jhenderson@hunton.com