Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 4 April 2013

The EU Article 29 Working Party Opinion on Apps on Smart Devices and its Implications

By Daniel Cooper and Oliver Grazebrook, of Covington & Burling LLP, London.

Introduction

The EU Article 29 Data Protection Working Party's (the Working Party) Opinion 02/2013 (the Opinion) on apps on smart devices, which was adopted February 27, 2013, and made public March 14, 2013, aims to clarify the legal framework of a hitherto largely unregulated area (*see WDPR, March 2013, page 35*). The close interaction between the user and the operating system allows apps to access significantly more data than a traditional internet browser. This includes a large variety of personal data, including contacts, location, browsing history and financial information. This proliferation of data collection has created multiple risks to the private life and reputation of users of smart devices.

The Opinion follows an investigation by the Canadian and Dutch data protection authorities (DPAs) into the messaging app "WhatsApp." During the investigation, it emerged that WhatsApp was not obtaining consent from a large proportion of users before accessing their contacts, which was deemed to breach both Canadian and Dutch data protection laws (*see WDPR, February 2013, page 36*). The Opinion has confirmed that this is an area that DPAs are increasingly concerned about.

The Working Party highlights several causes of potential risk, including the "fragmentation" between different parties in the app development ecosystem, a lack of transparency and awareness for users, and an apparent trend towards data maximization and elasticity of purpose.

In order to address these issues, the Working Party has set out clear guidelines in several key areas. These include a clarification of which parties are data controllers for the purposes of data protection legislation, and suggested measures to combat fragmentation. Furthermore, the Working Party has provided detailed guidance regarding consent and notice for users, data minimization and purpose limitation.

This article analyzes the Working Party's views in these key areas, and discusses potential consequences for the various parties in the app development ecosystem.

Although this Opinion will be welcomed by smart device users, the app development industry may be less pleased. Applying the Working Party's guidance will be onerous, and will require a shake-up of the way in which apps are delivered to users. This process will require thorough consideration and innovation, both in terms of the app's codebase and the app industry's business models. The app developers must also take care that any changes do not result in a deterioration of the end user experience.

Different Parties in the App Industry

Who is a Data Controller?

One of the Opinion's key areas of clarification regards the question of who can be a data controller in the context of apps, and thus be subject to data protection legislation.

The Working Party confirms that app developers, app stores, operating system (OS) and device manufacturers, and third parties such as advertisers can all be considered data controllers as defined in Article 2(d) of the EU Data Protection Directive, to the extent that they determine the purposes and means of the processing of data on smart devices. Furthermore, these parties do not necessarily have to be located in the European Union; the Working Party confirms that any parties that target EU users will be covered by the EU legislation.

This broad application of the data controller role will force many parties, who may not have previously considered EU data protection, to review their practices. For example, the Working Party does not differentiate between the roles of app developer and app publisher. This means that, hypothetically, a small American startup company, developing apps for bigger corporations that publish apps in the European Union, would be expected to be just as compliant with EU data protection law as the publishing corporations. In practice, it will be interesting to see how strictly the EU DPAs choose to apply these suggestions.

Dealing with Fragmentation

In addition to confusion regarding data controllers, the large number of different parties in the app ecosystem also raises security concerns.

In order to tackle the security issues caused by this fragmentation, the Working Party calls for greater cooperation between the parties. For example, the Working Party recommends that app developers work together with OS and device manufacturers to develop innovative solutions for adequately informing users about data processing on mobile devices.

Undoubtedly, a greater level of awareness of the various parties in the network, and of how they interrelate with each other, would be a positive step. As the Working Party states, "the chain of multiple actors is only as strong as its weakest link." An app developer may utilize the services or software of any number of processors, and if those processors are lacking appropriate data protection mechanisms, user data may be compromised, regardless of the data controller's practices. Furthermore, the data controller will be liable for any shortcomings of the processors. In keeping with this focus on awareness of the multiple parties, the Working Party also calls for app developers to make users aware of any processing undertaken by third parties on their behalf.

However, on occasion, the Working Party seems to go further than recommending cooperation and awareness, and appears to pass responsibility for app developers' compliance with data protection legislation onto app stores and OS and device manufacturers. For example, the Working Party states that OS and device manufacturers should develop application programming interfaces (APIs) that provide precise controls on the different data to which apps can have access. As another example, the Working Party also states that app stores *must* "enforce the information obligation of the app developer, including the types of data the app is able to access and for what purposes, as well as whether the data is shared with third parties." Commentators have compared this imposition of a "gatekeeper" role to the provisions of the proposed Stop Online Piracy Act in the United States, which proposed to impose responsibility for intellectual property infringement on internet service providers (ISPs), and, as a result, received a widespread negative reaction from ISPs. Therefore, we may see a pushback against these suggestions from OS and device manufacturers and app stores, who will argue that app developers should be responsible for themselves.

Informed Consent, Data Minimization and Purpose Limitation

Clarification of the Law

In the context of apps, consent is key for data controllers to comply with both the Data Protection Directive (consent for processing personal data) and the EU e-Privacy Directive (consent for placing information on the device or accessing data stored on the device). Both forms of consent must be free, specific, and informed. For consent to be "freely given," users must have the option of refusing the processing of personal data. To be informed, "the data subject must have the necessary information at his disposal in order to form an accurate judgment." Finally, to be specific, "the expression of will must relate to the processing of a particular item or a limited category of data processing."

Furthermore, the Working Party notes that, even if consent has been obtained, the data controller must still make sure that any processing is not excessive or disproportionate. This means adhering to the principles of purpose limitation and data minimization. This means that any data processing should be limited to the purpose for which the app was designed. The Working Party provides the example of an alarm clock app, which could process verbal commands for the purpose of running a voice-activated "snooze" function, but should not otherwise record sound. If an app developer wishes to process data for purposes that are not clearly linked to the purpose of the app, users should be kept informed and have the opportunity to withdraw their consent.

Current State of Affairs

Currently, users generally click an "install" button prior to installation of an app, although the option to do anything other than "accept" is rarely available. This consent is unlikely to be "freely given," in accordance with the Working Party's Opinion 15/2011 on the definition of consent (*see analysis at WDPR, August 2011, page 4*). Furthermore, it is even rarer for an app to offer specific

   ISSN 1473-3579

or granular consent; rather, many providers often treat the pre-installation acceptance as an invitation to take as much data as they can, for any purpose. There is also currently a distinct lack of available information for users. The pre-installation acceptance screen may often provide a list of vague purposes for processing, such as "market research." Finally, the Working Party observes that the majority of paid apps do not currently have a privacy policy.

Proposed Solutions

It is unlikely that current practices will be able to continue unaltered, but the transition period will not be easy, and the various parties shall have to strike a balance between giving users the means to control their privacy more effectively, and making systems that are too complicated and lead to user dissatisfaction. A clear first step is for app developers to draw up privacy policies. The Working Party cites this as a "minimum transparency requirement." A detailed privacy policy would provide information for users who want to know more, but would not interrupt the user experience.

Another suggestion made by the Working Party is the use of layered notices, in which initial notices provide the minimum required information but contain links to more detailed information. This prevents the user from being faced with a large volume of highly detailed information, which can be hard to digest.

Another potential option for app developers wishing to comply with the requirement for specific and granular consent is the use of "just-in-time" notices. These in-context pop-ups would warn users prior to processing that an app is about to process data for a particular purpose. This would provide a much higher level of transparency for users than agreeing to a long and broadly worded disclosure prior to installing the app. It would also allow app developers to inform users about updates to the app, and any additional types of data processing that may come with the update. If the further processing will be for a purpose that is markedly different from the purpose to which the user originally consented, the "just-in-time" notice could also be used as a mechanism to gain further consent (or to provide an opportunity to opt out). This would comply with the principle of purpose limitation.

However, these are not perfect solutions. Firstly, there is the problem of how to convey detailed and comprehensive information on a small screen, an issue that the Opinion touches on. Secondly, although frequent pop-ups may be welcomed by some privacy conscious individuals, many users will find them annoying. The various parties will not want to jeopardize their businesses by driving away a large cross-section of their target market.

Although, as mentioned above, other parties may be unwilling to cooperate in solving what they might see as largely an app developer's dilemma, the Working Party is right in suggesting that this problem will be best solved if the various parties work together. For example, OS and device manufacturers could work together with app developers to create control systems that give users granular control over what data they are happy for apps to process. Firstly, it should present the user, in an easily digestible format, with the types of data that the apps could potentially access and process. Secondly, it should provide a mechanism for the user to be able to easily opt out of the processing of certain categories of data.

This solution proposed above would seem to weigh heavily on the side of user privacy. Many app developers' business models are based on their ability to take advantage of "data maximization." Without access to such a rich mine of data, app developers may start to see a decline in profit. Thus, if this Opinion does lead to a shake-up in the way apps deal with privacy issues, app developers may have to seriously rethink their business models. Those who object to having their data processed may find that they have to start paying more for apps, as app developers, who find themselves unable to exploit user data as easily as they once could, may be less willing to offer their apps free of charge.

Conclusions

As stated above, the Working Party has cast a wide net over an industry in which many of the key players may not have considered data protection issues before, possibly not realizing that they were "data controllers," or purposefully ignoring data protection legislation, due to the lack of concern shown by relevant authorities. With the publication of this Opinion, the various parties in the app development ecosystem can no longer sit by and plead ignorance. Although the Working Party's Opinions are not binding law, this Opinion makes it clear that data protection laws apply to apps.

The EU DPAs likely will give the industry time to react before they start taking any action against offenders, thus placing the ball temporarily in the app industry's court. Some of the more straightforward propositions, such as ensuring a greater awareness of the different "links in the chain" and drawing up privacy policies, should be adopted in due course as matters of good practice.

However, time will tell whether the various parties choose to take on the more ambitious recommendations, such as the demand for more innovative ways of gaining informed consent, as these measures will no doubt require more thought to get right and may entail a reduction in data collected.

App developers in particular must decide how much control they are willing to cede to users, and then the optimal method for doing so. However, as the recent investigation by the Dutch and Canadian DPAs into WhatsApp's privacy practices shows, these are issues with which DPAs around the world are increasingly concerning themselves, and the app industry should choose to act sooner rather than later.

The Article 29 Working Party's "Opinion 02/2013 on apps on smart devices" is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

Daniel Cooper is a Partner with Covington & Burling LLP, London, and counsels clients on EU and UK data protection, data

retention, and freedom of information laws, as well as associated information technology and e-commerce laws and regulations. He may be contacted at dcooper@cov.com. Oliver Grazebrook is a Trainee Solicitor in the firm's London office, currently undertaking second seat in the Tech & Media practice group.

  WDPR ISSN 1473-3579