BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:58
To: Verweij, Ellen
Subject: FW: TechAmerica Europe Comments on pseudonymous data and profiling
Attachments: TAE Comments for DAPIX on specific issues of Chs I-IV-final.pdf

Follow Up Flag: Follow up
Flag Status: Completed

From: BRE-JUS
Sent: woensdag 15 januari 2014 14:01
To: Grave, Martijn-de; Ruiter, Mieneke-de; Dam, Caroline-ten; Alink, Marnix; Kaai, Geran; Timmermans, Marieke; Sorel, Alexander; Luijsterburg, Sander; Bos, Nicoline; Zwart, Jan
Subject: FW: TechAmerica Europe Comments on pseudonymous data and profiling

---

Van: [redacted]
Verzonden: woensdag 15 januari 2014 14:00:34 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Aan: [redacted]
CC: [redacted]
Onderwerp: TechAmerica Europe Comments on pseudonymous data and profiling

Dear DAPIX member,
(in 'cc: [redacted] Adobe – Chair Security & Privacy WG; [redacted] Google – Issue-Leader Data Protection)

Please find attached a **paper** that we have put together in response to the 19 December 2013 Presidency paper summarising the discussion on the concepts of **pseudonymous data and profiling** within DAPIX.

Please don't hesitate to contact us, should you have any questions.

Best regards,

[redacted]

EU Security and Privacy Policy Manager
TechAmerica Europe

TechAmerica EUROPE

Rue de Namur 16
1000 Bruxelles
Belgium

mobile: +32 (0) [redacted]
e-mail: [redacted]
website: http://www.techamerica.org/
linkedin: [redacted]

[redacted]

EUROPE
TechAmerica

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

TechAmerica Europe comments for DAPIX on Pseudonymous Data and Profiling as per 19/12/2013 paper on Specific Issues of Chapters I-IV

Brussels, 14 January 2014

TechAmerica Europe *represents leading European high-tech operations with US parentage. Collectively we invest Euro 100 bn in Europe and employ approximately 500,000 Europeans. TechAmerica Europe Member companies are active throughout the technology spectrum, from software, semiconductors and computers to Internet technology, advanced electronics and telecommunications systems and services. Our parent company, TechAmerica is the leading tech association in the US.*

This paper has been put together in response to the 19 December 2013 Presidency paper summarising the discussion on the concepts of pseudonymous data and profiling within DAPIX. Please contact Christian Wagner ([redacted]) for more details.

Introduction

TechAmerica Europe (TAE) welcomes the opportunity to comment further on the concepts of pseudonymous data and profiling, currently under discussion with in DAPIX. The June 2013 Irish Presidency draft of Chapters I-IV of the Regulation made significant progress on both these concepts, but the 19 December Lithuanian Presidency paper highlights a number of ongoing issues that need addressing before both concepts can contribute to an improved legal framework for data protection in Europe.

We believe much of the ongoing confusion about the concept of pseudonymous data derives from the fact that while some stakeholders – e.g. internet-based industries - see pseudonymous data as a concept that describes ***a particular state of personal data***, other stakeholders particularly in the medical and scientific research community prefer to speak of pseudonymisation to describe a ***process of de-identification***. Understanding these differences and resolving the confusion that these approaches cause will be essential if Council is to deliver on its promise to develop an effective risk-based approach within the new Regulation that can effectively calibrate controllers' and processors' data protection obligations while maintaining protection levels.

Commentary

Should delegations support the compromise reached in Irish presidency document (11013/13), namely the definition of "pseudonymous data" and corresponding calibrations of specific provisions of the draft Regulation?

Yes, the definition of pseudonymous data is an essential concept to a modernised data protection framework; however there is room for improving the compromise text and the possibility of including a notion of pseudonymisation, understood as a representation of a "privacy by design" technique.

The June 2013 Irish text, while not perfect, contained a number of significant advances over the original proposal which merit the support of Council. We welcome, in particular, the inclusion for the first time of a definition of pseudonymous data, establishing the principle that not all identifiers may identify a data subject to the same degree and that different obligations might apply to the processing of such data. This is an absolutely critical insight and one of the cornerstones of any meaningful risk-based approach. We also welcome the reference to the use of pseudonymous data as an example of a relevant technique in the context of data protection by design (Article 23(1).

However there are areas where we believe the Irish compromise requires further development. In an information economy, data controllers need to be able to target content and differentiated offerings in response to unique identifiers without the law concluding that the controller has "identified" the person just by treating them differently. Pseudonymous data, in other words, should serve as a safe means of allowing data controllers to treat different data subjects differently without linking that data to conventional identifiers that allow for direct identification. But it is not clear from the presidency's use of the phrase "specific data subject" whether "specific" means an identified data subject or simply a data subject that has been distinguished from another without identification. If the definition were taken to mean the latter, then this wording would appear to preclude the attribution of information to any singled-out individual, even absent conventional identifiers.

In practical terms this distinction is important because, for example, websites aim to respond to information they gather about each unique, but unidentified, visitor to customise the experience for that visitor. The ability to safely tailor experiences on the basis of unique identifiers as a means of encouraging visitors to voluntarily directly identify themselves to a website is critical to the dynamics of e-ecommerce. But there is a risk that the Presidency definition of pseudonymous would not allow for this.

An amendment to clarify that the definition covers unauthenticated users to allow differential treatment (subject to appropriate controls), would be beneficial in terms of stimulating data minimisation.

Elsewhere, Recital 45 and Article 10 of the Irish Presidency text actually contradict each other, with the recital focused on processing that *permits* identification while the Article considers processing that *requires* identification. The change of focus in the Article is a significant change to the original European Commission drafting which, we believe, contradicts the original intention of that Article which was to help controllers who wish to treat unique users differently even if they could not then isolate the real person behind the online profile. The notion that processing should not "require" (as opposed to permit) identification is problematic because the notion of identification covers both direct and indirect identification. It is likely that much processing might *require* some form of indirect identification (i.e. to allow for customized experiences for two unique but unidentified visitors) but without *permitting* direct identification. If processing requires indirect identification then the

controller could in theory be required, under the presidency draft, to acquire more information to identify a visitor so that they are distinct from every other visitor.

A return to the original Commission drafting, or the extension of the language of Recital 45 into Article 10, is required.

We also have concerns with the implications of Recital 39 (which allows that the processing of personal data for the purposes of anonymising or pseudonymising personal data can be considered as a legitimate interest of the controller). On the face of it this attempts to provide legal coverage for situations where a controller collects but quickly anonymises or pseudonymises personal data. While in theory this could help avoid splitting legal hairs over how fast anonymisation / pseudonymisation must take place (is 1 millisecond too slow?), the approach risks creating further legal uncertainty that undermines the legitimate interest clause. Pseudonymisation is not a *purpose* in itself. It may be a feature of a privacy by design approach, as the Irish presidency correctly identifies. And it may be a step in the processing of data for some other purposes (which may be pursued on various legal bases including legitimate interest in certain contexts). But pseudonymisation says nothing of the lawfulness of data collection in the first place, or of the lawfulness of subsequent processing.

Article 30(1) should refer to pseudonymisation rather than pseudonymous data. As with privacy by design, pseudonymisation is a technique that can support the secure processing of data.

Delete the reference to pseudonymous data in Article 32(2)a. The derogation from breach notification requirements for pseudonymous data overstates the protection offered by pseudonymous data. It should be remembered that this is not the same as anonymous data (which implies that someone would require a disproportionate amount of time or effort to identify an individual) or even encrypted personal data, but simply data that cannot identify an individual without additional data. When a breach occurs it cannot be known if the party that obtains the pseudonymised data has the necessary data to re-identify the individuals.

Should the definition of "pseudonymous data" be replaced by a reference to a process supporting compliance with data protection requirements of the Regulation ("pseudonymisation")?

No. The concept of pseudonymous data cannot and should not be replaced by that of pseudonymisation. The legitimate business models of many stakeholders are not well served by a framework that fails to accommodate both pseudonymous data as a state and pseudonymisation as a process.

While the personal data definition proposed by the European Commission largely repeats concepts which exist within the existing Directive (reasonableness test, ability to identify, direct and indirect identification) it *does* increase uncertainty on the status of an extended range of identifiers which may or may not, depending on the circumstances, be personal data. This has been done, inter alia, to respond to ECJ jurisprudence, e.g. *Sabam v Scarlet* which states that for example IP addresses are "protected personal data", albeit referring only to the specific context of a data controller allocating that IP address to a known subscriber.

TAE members agree that such identifiers are worthy of protection and are rightly in scope for the Regulation. However we believe the Regulation needs to provide more efficient mechanisms for distinguishing between all types of personal data across the entire spectrum from clear direct identifiers to data which can only hypothetically or with a significant effort and cost be linked to a data subject. **The introduction of pseudonymous data as a subset of personal data would allow for an injection of a risk-based approach where it is most needed, and in a way which is entirely consistent with ECJ jurisprudence and the EU principles of necessity and proportionality. Failure to do so would leave data controllers confronted with the lack of legal certainty of Recital 24.**

A workable definition of pseudonymous data must therefore be flexible enough to cover both (i) data that has once directly identified an individual and has undergone a process to render it less likely to identify that person, and (ii) a series of unique online identifiers gathered about a data subject which may never have reached the point of actually allowing a controller to identify the person behind the data. Medical research tends to fall into (i) while internet industries rely on (ii).

If a single definition cannot be found that covers both of these, then a separate additional definition of pseudonymisation (to describe a process of de-identification) is needed to provide legal support for the further processing of data for purposes including medical and scientific research. This definition could in turn be referenced in Article 24 on privacy by design as an example of a process which can help data controllers protect the interests of data subjects.

Profiling

Should delegations support the current compromise text on the issue of "profiling"?

Should the definition of "profiling" be kept as in the current compromise, be identical to that of the Council of Europe; or remain in line with the logic of Directive 95/46/EC?

We believe that the alternative definition of profiling outlined by the presidency in Paragraph 9, which seeks to align the definition of profiling with the logic of Directive 95/46/EC, should be supported. This point aside, the overall approach to Article 20 in the Irish presidency compromise text should be supported.

On the definition of profiling, we agree with the argument outlined in paragraph 9 that this definition offers protection to a broader range of data by not requiring the creation of a profile. This approach is also more technology neutral and is hence less likely to be rendered obsolete by technological development.

Data processing has substantially advanced since 1995. The ability to process data to extract new actionable insights is now absolutely essential to a knowledge-based economy. So any changes in Article 20 need to effectively protect the data subject against automated decisions that impact their legitimate interests whilst allowing legitimate and beneficial business activities that use advanced data processing techniques to continue and contribute to growth, jobs, entrepreneurship, innovation and competitiveness in Europe.

One of the ways that the Irish presidency compromise draft does this is by addressing a broader range of aspects than Article 15 of the 1995 Directive, such that location, behaviour and personal preferences are all now included. This means that data subjects that are subject to automated decisions based on these aspects and which affect their interests in a particular way are now entitled to some form of human intervention. The Irish compromise text ensures further welcome protections for data subjects compared to the current Directive by outlawing the use of profiling based on sensitive categories of data without suitable safeguards. It also effectively considers profiling as a separate category of data processing by limiting the legal bases available for such processing, compared to normal data processing. (NB This is in addition to the standard right to object to any data processing that is based on the legitimate interests of the data controller enshrined in Article 19). **These are all measures that ensure strong protection for data subjects and represent welcome extensions of Article 15 of Directive 1995/46/EC.**

Furthermore, we welcome in particular the fact that the compromise text has strengthened the legal threshold for impact on a data subject from "significant effect" to **"severely affects"**. The proposed threshold also reflects a harm-based approach encompassing the requirement for a negative effect on the data subject. This is a pragmatic move that should reduce the likelihood of many legitimate business practices (particularly from the e-commerce space) being subject to unnecessary restriction. Some commentators have, for example, suggested that the targeting of content to unique but not identified website users, for example, should be considered as having a "significant effect" and thus be subject to Article 20. We reject this idea, and believe that the intention of Article 20 is to focus on clearly unfair or discriminatory practices such as the denial of insurance cover. A lower threshold could easily result in prohibiting many beneficial data processing techniques and enabling technologies across sectors that are clearly not intended to be covered by this provision. **Absent this change in threshold, then it would be necessary to introduce the legitimate interests of the data controller as an allowable legal basis into the text of Article 20(2) to ensure a better balance of interests between data controllers and data subjects.**

Overall, when considering Article 20, it is important to reflect on the issues that the provision is attempting to address. Article 15 of the current Directive does not *prohibit* automated decisions, but rather seeks to ensure that human intervention is possible when automated decisions are taken that affect individuals in a particular way. Decisions that have a legal effect or significant effect are still permitted provided safeguards, such as the right to obtain human intervention, are in place. It is important that this concept is maintained in Article 20.

For further information please contact: [redacted]
EU Security & Privacy Policy Manager
Rue de Namur 16
1000 Brussels
[redacted]

[redacted]