MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGHAI,
SINGAPORE, TOKYO, WASHINGTON, D.C.

January 23, 2018

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

Submission from the Global Privacy Alliance to the Article 29 Data Protection Working Party on Guidelines on Transparency under Regulation 2016/679

The Global Privacy Alliance (GPA) welcomes the opportunity to comment on the Guidelines on Transparency under Regulation 2016/679 ("Guidelines") issued by the Article 29 Working Party ("Working Party").

The GPA is comprised of a cross section of global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, medical devices, pharmaceutical, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

The General Data Protection Regulation (GDPR) requires transparency with respect to the processing of personal data. As the Guidelines explain, this obligation applies to the provision of information to individuals related to the fair processing of their personal data, how data controllers communicate with individuals regarding their rights under the GDPR, and how data controllers facilitate the exercise of those individuals' rights. The Guidelines provide some helpful examples of the types of information that an organization may need to provide to meet its transparency obligations under the GDPR. However, we have concerns about the level of detail that the Working Party is recommending with respect to data recipients, third country transfers, balancing test information, and user panels. Moreover, some of the specific comments from the Working Party seem to expand the meaning of the GPDR in ways which make compliance substantially more difficult without adding additional privacy benefits to individuals.

I. Naming Individual Recipients

Articles 13.1(e) and 14.1(e) of GDPR require that individuals be provided with information on the recipients or categories of recipients. However, in the Schedule to the Guidelines, the Working Party states that "the default position is that a controller should provide information on *the actual (named) recipients* of the personal data. *Where a data controllers opts only to provide the categories of recipients, the controller must be able to demonstrate why it is fair for it to take this approach*… information on the categories of recipients should be as specific as possible by indicating the type of recipient, the industry, sector and sub-sector and the location of the recipients."

We believe that this proposed approach goes beyond the requirements of the GDPR, raises serious security concerns and does not substantially enhance the privacy protections afforded to individuals. Companies often use service providers as a way of providing better security for their data. Part of the assessment involves using a variety of service providers so that all of the company's most important data is not all in one place. Making public such detailed information of the identity and location of the recipients would give bad actors information on where exactly to find an organizations data and a road map of the vendors that are likely to have the most valuable data. Moreover, multinational companies engage hundreds of service providers for varying periods of time. Their list of service providers and their geographic location is constantly changing. Requiring companies to notify individuals regarding the location of service providers accordingly in order to meet their transparency obligations under the GDPR imposes an enormous administrative burden and does little to enhance individuals' privacy rights. In addition, the GDPR and the Working Party emphasize the goal of having notices that are short and easy to understand. Listing each and every service provider is contrary to that goal.

Identifying the categories of service providers and affirming that such providers offer sufficient guarantees to process and protect the information in accordance with the GDPR would provide individuals with meaningful information about the processing of their personal data without exposing the company to unnecessary security risks. Identifying the categories of service providers should remain a valid means of meeting this requirement.

II. Listings Of Third Country Transfers

In the Schedule in the Guidelines, the Working Party states that in accordance with the principle of fairness, the information should explicitly mention all third countries to which the data will be transferred. Particularly for a large multinational company that likely transfer some personal data to all of the countries in which they operate, this requirement seems pointless and does little to advance the individual's private rights. For example, a large multinational may have a global employee directory. If the company operates in 50

countries, then consistent with the guidance, the notice would need to include a list of 50 countries. Similarly, if a company outsources its customer services operation to provide 24/7 services, it would have to list all of the countries that might answer a support call or might provide service. Individuals are concerned that their information is properly protected, not whether the company is operating a call center in the Philippines or in Malaysia. It should be sufficient to notify individuals that their personal data is being transferred to countries, some of which may not be recognized as providing adequate protection and in such cases, advising that the company has appropriate safeguards in place that satisfy GDPR requirements.

III. Information From The Balancing Test

Where a data controller relies on legitimate interests as the basis for its processing (Article 6(1)(f)), the GDPR (Article 13(1)(d) requires the data controller to provide individuals with information about the specific legitimate interests being pursued. The Guidelines further recommend, as a matter of best practice, that the data controller provide individuals with "the information from the balancing test, which should have been carried out by the controller to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data."

Consider the following employment example. A company wishes to centralize its employee data processing in order to conduct work force analytics, ensure fair and consistent compensation across the organization, assess hiring needs, and carry out succession planning. Besides stating what they company is going to do with the data, it is not clear what additional information can be provided that would be useful to individuals or in any way privacy enhancing. Therefore, we think the Working Party should clarify that provision of information from the balancing test is not required and recommended only on an exceptional basis.

IV. User Panels

According to the Guidelines, "Controllers can demonstrate their compliance with the transparency principle by testing the intelligibility of the information and effectiveness of user interfaces/notices/policies etc. through user panels." (page 8).

While reliance on user panels may make sense for large consumer companies that have direct interaction with individuals, deployment of such panels in the B-B context, particularly for small or medium sized businesses, it is not helpful and would impose an unnecessary administrative and cost burden. Therefore, we think it would be helpful for the Working Party to clarify that this option will be less appropriate for B2B companies.

V. "Disproportionate Effort"

On page 27 (para. 55) the Guidelines limit the use of the Article 14 "disproportionate efforts" provision beyond what is contemplated by the Article or its recitals. This limitation could seriously harm the public interest and lead to information overload of notices to data subjects pursuant to Article 14. The Guidelines conclude that "the exception cannot be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes."

That conclusion inappropriately takes the "examples" from GDPR Recital 62 and makes them the only contexts in which the disproportionate efforts principle can be invoked. That would impede the use of collected data for lawful purposes such as confirming identity or fighting fraud, terrorism, and money-laundering. Many services used for these purposes on a legitimate interest legal basis involve data indirectly obtained about individuals. This is not archiving for research or similar purposes. Yet any interpretation of Article 14 to require that notices are sent to every single individual having data in such services would either render these critical services too expensive to be used, overwhelm individuals with notices, or alert "bad actors" by omission that they are not on a watch list and may proceed with criminal plans. Recital 62 confirms that the number of individuals can be a key factor in whether to apply the disproportionate efforts exception in Article 14.

We recommend deletion of the conclusion that the disproportionate efforts clause cannot be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes.

VI. Use Of The Terms May, Might, Often Or Possible

The Guidelines discourage the use of terms such as "may," "might," "often," and "possible." While certainty is always preferred, what information an organization will collect or how it will be used is often contingent on the choices made by the user.

For instance, if a user elects to participate in a prize draw or contest, then certain information may be collected. How well the individual does in the contest will change what information is collected. Thus it is accurate to use the conditional to describe the information that might be collected or may be needed because at the time of the notice it is unknown what the individual will elect to do.