June 2015

On the Death of Purpose Limitation

By Lokke Moerel and Corien Prins

This article originally appeared on the IAPP's Privacy Perspectives.

The latest Council version of the European General Data Protection Regulation (GDPR) provides that personal data may be further processed by the same data controller even if the further purpose is incompatible with the original purpose "if the legitimate interests of that controller or a third party override the interests of the data subject." The Article 29 Working Party (WP29) and a large number of non-governmental organisations have expressed concerns that this would render the fundamental principle of purpose limitation meaningless and void.

Is this indeed correct? We do not think so.

We feel that the approach of the Council is the only feasible way to guarantee protection given that it is much better suited to deal with developments such as the Internet of Things (IoT) and big data.

Let us explain.

The *purpose limitation* principle consists of two elements:

- data must be collected for specified, explicit and legitimate purposes only (*purpose specification*); and
- data must not be further processed in a way that is incompatible with those purposes (*compatible use*).

The purpose limitation principle has served as a key principle in data protection for many years. In today's data-driven society, however, the purpose limitation test has become outdated as a separate test. Imagine a mobile app that on a real-time basis records our health data, predicting how we'll feel the next day and where to avoid getting the flu. Perhaps pushing the bounds of creepy, this app, however, may be of great value for the World Health Organisation (WHO) to protect civilians from life-threatening infectious diseases.

These two apps collect and use data for the same purpose, namely mapping and predicting health and illness, but our assessment of the two apps is totally different.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Kimberly R. Gosling (858) 314-5478
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
Stephanie Sharron (650) 813-4018
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346
Lokke Moerel 44 20 79204054

Brussels
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Susan McLean 44 20 79204045
Alex van der Wolk 44 20 79204074

ASIA

Beijing
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

The commercial application will not automatically gain societal acceptance, while most of us would see the value of the second application. Whether personal data may be collected and used by such a mobile app is not so much based on the purpose for which the data is collected and processed but on the interest that is served.

As such, we conclude that for data collection and further processing of data, a test based on the legitimate interest is better suited in today's data-driven society than the current test based on the initial purpose for data collection and whether further processing is compatible with such initial purpose.

Note that with this we do not argue that data limitation or minimisation is no longer relevant.

On the contrary, this principle is still relevant, but in our opinion it should be tied in with the interest served rather than with the original purpose for data collection. This does not mean that more data may be collected and processed. Rather, it may well lead to less data being justifiably processed.

For the record, we are not in favour of a "use-based"" system, in which data collection is left unchecked. Without regulation of data collection, we would end up in a situation where governments and companies would collect rampant data.

The purpose limitation test has become outdated because, in the past, personal data was primarily a by-product of the purpose for which the data was collected. When we book a flight, we are requested to provide name, address, date of birth and bank account number. The data is a by-product of the service. The requirement of purpose limitation is an objective test to determine what data is justified for that purpose.

Today, with developments like the IoT, records are no longer a by-product of a purpose, but rather, the data is collected first in order to deliver the service—think smart homes and appliances.

The purpose and the collection of the data then coincide.

A similar issue arises when a company decides to collect and combine data from public sources in order to analyse the data and provide a new service. It is the company that decides on the service to be provided (on the purpose itself) which then justifies which data is required for such service. As a result, the purpose limitation test is no longer objective and is also non-limiting.

Most online web shops collect online visitor tracking information. While not all data categories collected are strictly necessary to provide access, it is very useful for the website owner to analyse how users behave in his web shop. This data enables the web shop owner to improve its services. Again, the purpose of collection coincides with the interests of the provider to collect the data.

We see these developments implicitly reflected in the opinions of the WP29. Traditionally, the WP29 first applied the purpose limitation test and assessed whether the controller had a legal basis to process the data. In its 2014 Opinion on the Internet of Things, however, the sequence of the tests has been reversed. First it tested whether the controller has a legal basis to process the data (in this case, the legitimate interest ground) and then the purpose limitation test is applied, no more data may be collected and processed than required for the relevant purpose as specified by the controller (which *de facto* equals the legitimate interest).

If this is how the rules should be applied, then let's make the system simpler by just applying the legitimate interest test to start with. In this system there will be one test for collection, use, further use and of which test the element of data limitation is already fully part.

Advocates of the purpose limitation principle will point out that this test contains more elements than discussed above, most notably the requirements that the purpose itself must be legitimate and be explicitly specified prior to processing. In its Opinion on the Legitimate Interest Ground, the WP29 indicated that the requirements for a legitimate purpose apply *mutatis mutandis* to the legitimate interest test, which include the requirement that the purpose must be specified before the collection and processing takes place. Our conclusion is that all elements of the purpose limitation principle are covered by the legitimate interest test. Here the purpose limitation test does not play a role, and therefore only has a role to play in respect of the other legal grounds, such as consent and contract.

Here is the elephant in the room.

Consent and contract are often misused for processing data that would not pass the legitimate interest test. These grounds in themselves do not require the balancing of interests, including the requirement to implement mitigating measures to minimise the impact on the privacy of individuals. In that respect, the legitimate interest ground is better suited and often provides more protection to individuals.

We feel that this is exactly the reason why the WP29 in its Opinion on Purpose Limitation considers relevant for the assessment whether there is a legitimate purpose, also "the general context and facts of the case," including "the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise." These factors are not foreseen in the legislative history of the Directive (which refers to an assessment of whether the processing is a violation of the law only). This seems to be an attempt of the WP29 to introduce the contextual analysis of the legitimate interest test also for the other legal grounds. The bottom line is that it results in three tests:

- whether there is a legitimate purpose;
- whether there is a legal ground (including the legitimate interest ground), and
- whether further processing is not incompatible with the initial legitimate purpose.

If the factors listed by the WP29 for each of these three tests are compared, each requires a full assessment of the facts and the context of the case, including the underlying relationship between controller and individual and the reasonable expectations of the individual. Of course, the differences between these tests may be understood by legal experts, but based on our personal experience, both as teachers to practitioners as well as working with companies on their privacy compliance, most people completely miss the point.

The rules are simply too complex and result in an atmosphere of ridiculing the rules instead of an attempt to comply. We are in urgent need of a simpler system. The time has come to recognise the legitimate interest ground as the main legal ground for each and every phase of the data lifecycle. The balancing act of the different interests at stake can then take into the mix whether a contract exists and only allow consent as a mitigating measure rather than predetermined grounds for processing.

Let us remember the important lesson from the First Report on the Directive, which concluded that the Directive was overly strict and complicated and that this is a recipe for non-compliance which in turn undermines the legitimacy of the material norms which these rules aim to protect.

Click here for the extended and annotated version of this article.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.