



EUROPEAN COMMISSION

Joaquín Almunia

Vice President of the European Commission responsible for Competition Policy

Competition and personal data protection

Check Against Delivery
Seul le texte prononcé fait foi
Es gilt das gesprochene Wort

Privacy Platform event: Competition and Privacy in Markets of Data
(Brussels)

26 November 2012



SPEECH/12/860

Ladies and Gentlemen,

I thank Ms In 't Veld for her kind invitation to join this meeting of the Privacy Platform initiative.

Privacy – and the many delicate issues associated with it – is becoming one of the central debates of our time.

Thanks to technological and commercial developments, growing amounts of information can be collected about individuals.

As a result, the ability and the incentive of companies to gather, manipulate and trade personal data have never been stronger.

Almost every day brings new, sophisticated methods to collect and process information from unsuspecting users.

Today, we are asked to submit personal information all the time. We cannot send flowers online or book a flight without giving away our names, addresses, and credit-card numbers.

Yet, only 18% of online shoppers think they are in complete control of their personal data.

In fairness, the treatment of personal data should not be demonised. Companies can use information about their clients to tailor a service to their specific needs.

But there is a delicate trade-off between privacy and better service and this is precisely why we need debates such as the one we're having today.

The respect of private and family life and the protection of personal data are much bigger issues than just a commercial debate.

In fact, they are freedoms enshrined in the Charter of Fundamental Rights of the European Union.

How are these fundamental rights implemented in the EU?

The main European law that protects the privacy of individuals with regard to the processing and free movement of personal data is the Data Protection Directive of 1995 and the national laws that implement it.

The Directive became operational when the internet was still in its infancy. Things have changed a lot since then. Today, 250 million people use the internet daily in Europe.

It is clear that the protection of personal data in Europe must evolve. Last January the Commission approved the draft for a broader and more robust Regulation to replace the 1995 Directive.

When the Regulation becomes operational, it will protect all EU residents even if their personal data are held by companies outside the Union; and it will ensure the 'right of portability' and the 'right to be forgotten'.

These important changes address a growing concern among Europeans. 70% of Europeans think that their personal data held by companies may be used for a purpose other than that for which they were collected.

The data-protection reform will help remove real and perceived barriers to the internal market by providing harmonized legal protection.

This will benefit consumers and companies alike. A stronger, simpler and clearer data-protection framework will encourage companies to get the most out of the digital Single Market.

When the new Regulation becomes operational it will foster economic growth, innovation and job creation – and it will do so at no cost.

Ladies and Gentlemen:

The rights I've just described protect us from the unwarranted access to our private data.

But the treatment of personal data has at the same time important implications for the Single Market – just think of e-commerce. The treatment of personal information is a booming industry.

Firms with legitimate businesses hold vast amounts of personal data and analyse them to detect patterns of behaviour for different categories of people.

This is valuable information for advertising companies and for entities that are interested in social behaviour. This covers the analysis needed for a variety of purposes such as electoral campaigns, surveys, market studies and so on. Today, personal data are a type of asset for companies.

We are aware that many companies collect vast amounts of personal data; such as telecommunication companies, payment systems, large retailers, and internet service providers – including social platforms.

We also know that these data are being matched and aggregated by yet another set of firms, and new challenges will doubtless arise with cloud computing and the trend towards storing and processing information remotely.

These fast and massive changes in the markets of data almost inevitably expose the industry to the risk of abuse. I understand there are and have been many cases of privacy violation involving a large number of firms.

Companies evidently try to use their access to personal data to gain commercial advantage vis à vis users.

It is necessary to strike the right balance between regulation and competition policy enforcement.

In my view, this sort of commercial abuses should be tackled first by a strong and effective consumer policy. Consumer policy will need to step up to prevent abusive access to private information and its commercial manipulation.

When unfair or manipulative commercial practices become pervasive in a market to the detriment of consumers and users the matter is best resolved with regulation.

But a more comprehensive regulatory process also allows a society to choose the balance it finds appropriate between privacy and commercial freedom.

This is a decision that we might not want to leave to markets because consumers are sometimes ill informed of the practices of merchants and may not have alternatives to turn to.

Competition policy is about tackling actions by a dominant firm to exclude competitors by unfair means. It is not well placed to tackle potentially abusive commercial patterns that can become pervasive in competitive markets.

This doesn't mean that competition policy should not be vigilant vis-à-vis the implications of the use of commercial data. A single dominant company could of course think to infringe privacy laws to gain an advantage over its competitors.

So far DG Competition has not had to handle cases where the accumulation or the manipulation of personal data were used to hamper competition.

The most prominent case involving personal data was the merger between Google and Doubleclick in 2008. This was a deal between a company that could collect a lot of personal data and another with the technology to target ads and monitor their performance.

Following an in-depth investigation, the Commission eventually cleared the transaction on competition-law grounds.

The analysis found no strengthening of dominant position in the search advertising services or in the advertising intermediation services that could be attributable to the merger. There were no merger-specific risks of foreclosure in any of these two markets.

The effect of the increase in the amount of personal information obtained by the merger entity was considered. The investigation found that the combination of information on search behaviour and web-browsing behaviour would not give a competitive advantage in the advertisement business that could not be replicated by other players that have access to similar web-usage data.

However, the decision made clear that it was clearing the merger "without prejudice to the obligations under EU legislation in relation to the protection of individuals and privacy with regard to the processing of personal data".

Apart from this case where personal data was analysed as an asset for the first time in a merger, our enforcement work has not had to tackle specific personal-data and privacy issues.

Although a company or a group of companies that would have exclusive access to personal data in a given market could give rise to concentration concerns, we have not encountered this situation yet.

For instance, we have not had to define a market for personal data or for any of its particular usages and we have not encountered a merger where we suspected that personal data could be used to keep competition at bay.

However, the fact that we have not encountered such a case in our enforcement does not mean that we can rule out the practice altogether.

In this respect, I believe that one of the principles of the current data protection reform goes to the heart of competition policy.

As I said, the proposed Regulation aims to ensure the 'right of portability'. This means that users should be able to move their personal data from one company to another without hassle and undue costs.

I believe that a healthy competitive environment in these markets requires that consumers can easily and cheaply transfer the data they uploaded in a service onto another service.

The portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them.

In those markets that build on users uploading their personal data or their personal content, retention of these data should not serve as barriers to switching.

Customers should not be locked in to a particular company just because they once trusted them with their content.

Whether this is a matter for regulation or competition policy, only time will tell.

Ladies and Gentlemen:

Let me sum up my arguments before I close.

Traditionally, the storage and treatment of personal data has been the province of laws and regulations designed to protect the privacy of citizens – and I believe that this will remain of paramount importance in the foreseeable future.

However, the commercial value of personal data has grown exponentially. In spite of this, DG Competition has yet to handle a case in which personal data were used to breach EU competition law.

But we cannot rule out this eventuality. In time, personal data may well become a competition issue; for instance, if customers were prevented from switching from a company to another because they cannot carry their data along.

I believe we are only at the beginning of a proper governance of privacy rights and of the commercial use of personal data.

A sensible treatment of personal data will allow us to benefit from better services targeted to our preferences and needs. But the line between the sensible use and the abuse of this kind of information is very thin. New problems will probably appear and become systemic.

There is clearly a trade-off here between risks and benefits. Is it wise to leave the search for the right balance to the individual? Can the market strike the right balance? Or perhaps it is better – and safer – to look for stronger regulatory solutions?

I will leave these difficult questions open to debate.

One thing I'm sure of is that we must find a way to preserve the right of all Europeans to a private and dignified life where their preferences, conversations and whereabouts are not systematically broadcast in cyberspace.

Thank you.