Uruguay Declaration
on profiling

Privacidad y tecnología en equilibrio

34° Conferencia Internacional de Autoridades de
PROTECCIÓN DE DATOS Y PRIVACIDAD

Punta del Este / Canelones, Uruguay - 26 October 2012

During their 34th International Conference held on 25 and 26 October 2012 in Uruguay, the data protection and privacy commissioners placed profiling at the centre of their discussions. This debate followed the discussions in Mexico City in 2011 on the ever growing amount of data being collected and processed by both private and public sector entities from around the world (the so-called big data).

We recognize the many useful applications of big data and the advantages large data collections could bring to, among others, healthcare, energy efficiency and public safety. However, at the same time the collection of personal information into large databases and the subsequent use presents risks to the protection of personal data and privacy. This is especially the case if large data collections are used for analysis and profiling in order to, among others, carry out risk analyses, which help organisations and companies to target persons. The risks become more pertinent from the moment profiling activities are carried out with data coming from various sources without taking due account of the quality of the data and the purpose for which they were first collected. We therefore reaffirm that the general data protection and privacy principles, most importantly the principle of purpose limitation, are and will remain the important framework on the basis of which processing operations should be judged.

Having heard the views of four experts in the field of profiling, with various backgrounds in both the public and the private sector, and the subsequent debate in the meeting it is our conviction that data protection and privacy commissioners should at least take the following items into account when dealing with profiling.

I. To create trust, public and private entities around the world need to ensure that they inform society to the maximum possible extent about their profiling operations. They should be more transparent about profiling, the way the profiles are assembled and the purposes for which the profiles are used. Providing better information should also ensure individuals have better control over their data.
II. Profiling operations need to be distinguished in three phases. First of all, it should be determined what is the need for the use of profiling. Secondly, the public or private entity in question should decide which assumptions and which data should form the basis for the profile. Finally, it should be decided in what way the profile can be applied in practice. It would be advisable if the various phases are subject to separate decisions and to regulatory oversight.

III. Both profiles and the underlying algorithms require continuous validation. This means controls should take place to verify if the results from profiling make sense and can reasonably be linked to the data provided at input. It also allows to further improve the profiles and underlying algorithms, thus improving results.
IV. Profiling operations should not take place without human intervention, especially now that the predictive power of profiling due to more effective algorithms increases. Injustice for individuals due to fully automated false positive or false negative results should be avoided.
V. The creation and application of profiles should preferably not be in the same hand. A balance needs to be found between the information used to create the profile and its practical application.
VI. Especially in the third phase, the practical application of the profile, provisions need to be established to allow the individual to challenge both the profile and the outcome.
VII. Profiling requires strong and independent privacy enforcement authorities with supervisory powers over both the public and the private sector. The authorities should ensure they have all the relevant and up to date knowledge regarding technological developments like profiling.
VIII. Governments have access to many large databases also containing data collected by private entities. Furthermore, they are able to create laws in order to define their own legal basis. Therefore, privacy enforcement authorities should be able to test and challenge government proposals, for example carrying out audits and be able to scrutinize in the pre-legislative phase.

Felipe Rotondo
Chairman of the Unidad Reguladora
y de Control de Datos Personales

Jacob Kohnstamm
Chairman of the Executive Committee
of the International Conference